# Cisco DNA Center for Industrial Automation Implementation Guide

First published: January 2022

Cisco Validated Design

Cisco Systems, Inc.  www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

# Contents

# Cisco DNA Center for Industrial Automation Implementation Guide

## Overview

The following is a complementary guide to the Cisco DNA Center for Industrial Automation Design Guide (https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Networking/DNA_Center_IA/DNA_Center_IA.html), providing configuration details associated with the respective design recommendations.

## Administration

### Installation

For information on installing the Cisco DNA Center appliance, refer to: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-installation-guides-list.html.

### Licensing

For this implementation the Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem) tool was used for Cisco DNA Center licensing. For Cisco SSM On-Prem installation, see: https://www.cisco.com/web/software/286285517/152313/Smart_Software_Manager_On-Prem_8-202006_Installation_Guide.pdf.

To link SSM with Cisco DNA Center:

1. From the Cisco SSM web interface, go to the **API Tool Kit** menu.
2. Under the **API Console** tab, click **Create** and choose **Resource Owner Grant** from the drop-down list.

**Figure 1 Cisco SSM API Tool Kit**

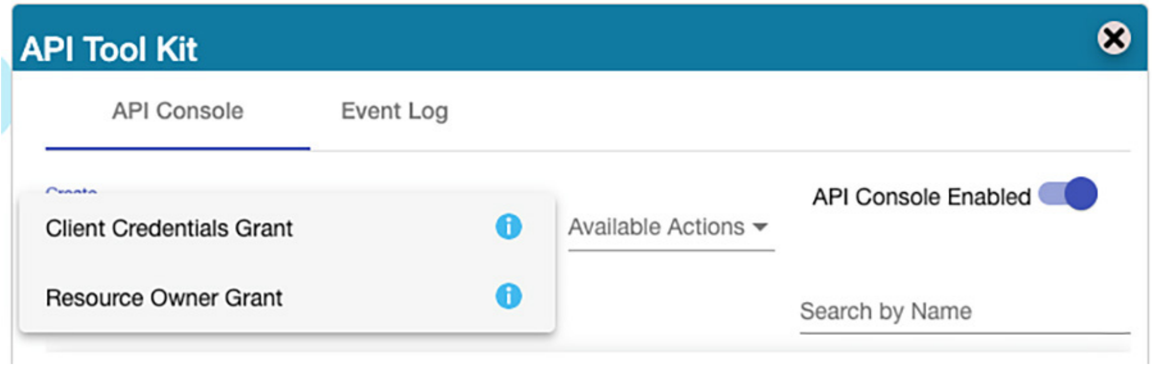
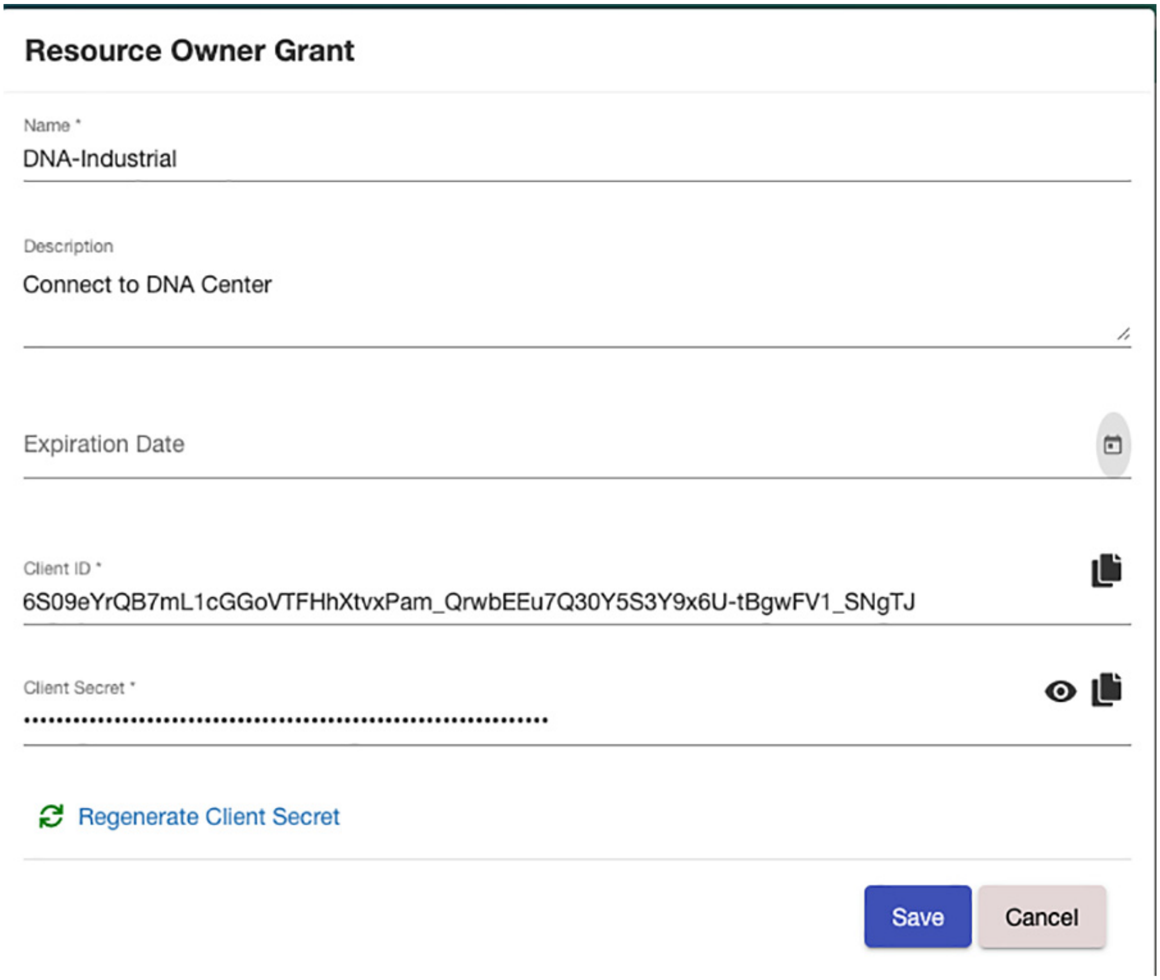


**Figure 2 Cisco SSM Resource Owner Grant**



Name *
DNA-Industrial

Description
Connect to DNA Center

Expiration Date

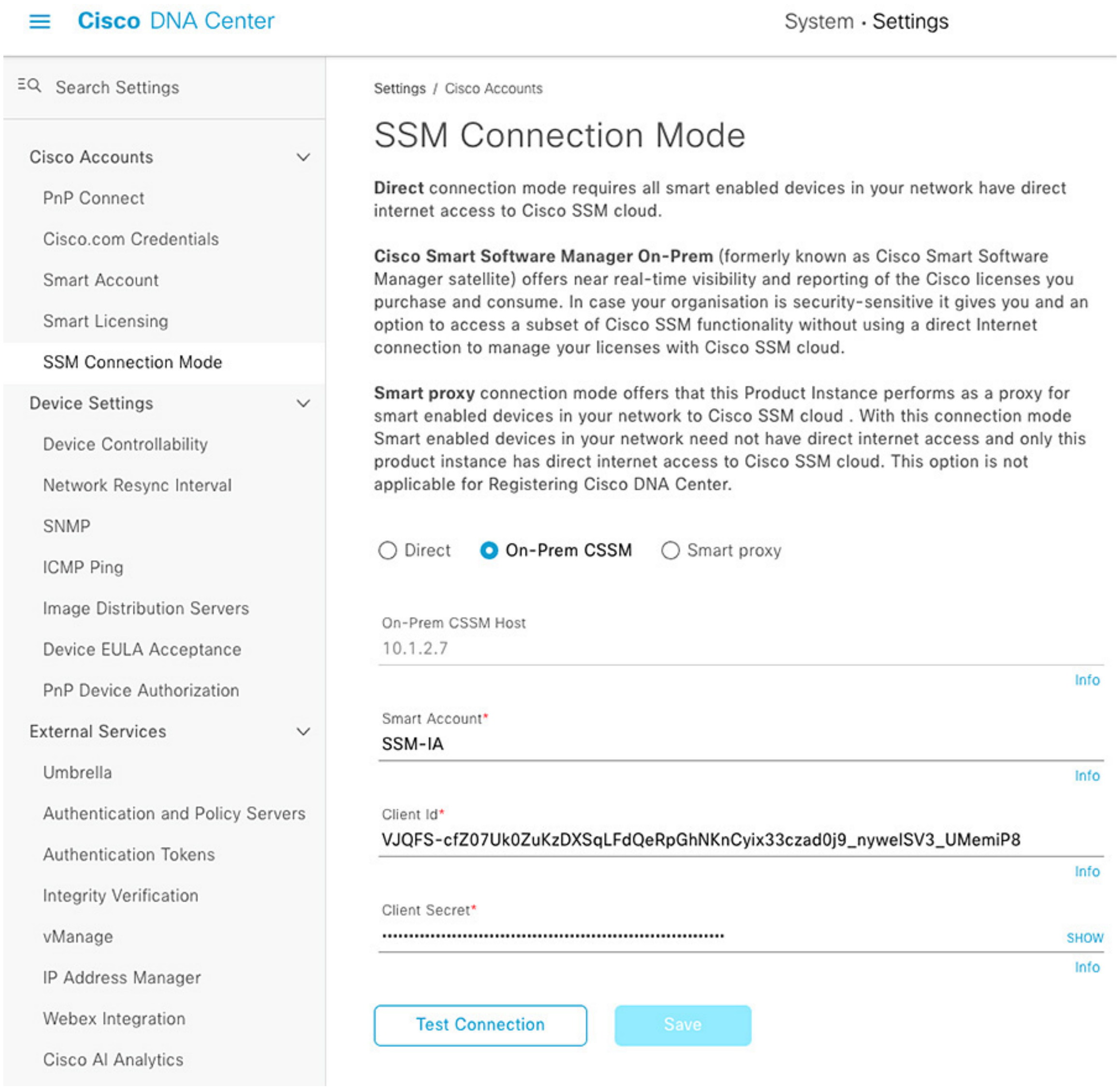
Client ID *
6S09eYrQB7mL1cGGoVTFHhXtvxPam_QrwbEEu7Q30Y5S3Y9x6U-tBgwFV1_SNgTJ

Client Secret *
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••

On Cisco DNA Center:

1. Navigate to **System > Settings** and under **Cisco Accounts** choose **SSM Connection Mode**.
2. Click the **On-Prem CSSM** radio button and enter the information from the SSM Resource Owner Grant.

**Figure 3 Cisco DNA Center SSM Configuration**



SSM Connection Mode

**Direct** connection mode requires all smart enabled devices in your network have direct internet access to Cisco SSM cloud.

**Cisco Smart Software Manager On-Prem** (formerly known as Cisco Smart Software Manager satellite) offers near real-time visibility and reporting of the Cisco licenses you purchase and consume. In case your organisation is security-sensitive it gives you and an option to access a subset of Cisco SSM functionality without using a direct Internet connection to manage your licenses with Cisco SSM cloud.

**Smart proxy** connection mode offers that this Product Instance performs as a proxy for smart enabled devices in your network to Cisco SSM cloud . With this connection mode Smart enabled devices in your network need not have direct internet access and only this product instance has direct internet access to Cisco SSM cloud. This option is not applicable for Registering Cisco DNA Center.

○ Direct ● On-Prem CSSM ○ Smart proxy

On-Prem CSSM Host: 10.1.2.7

Smart Account*: SSM-IA

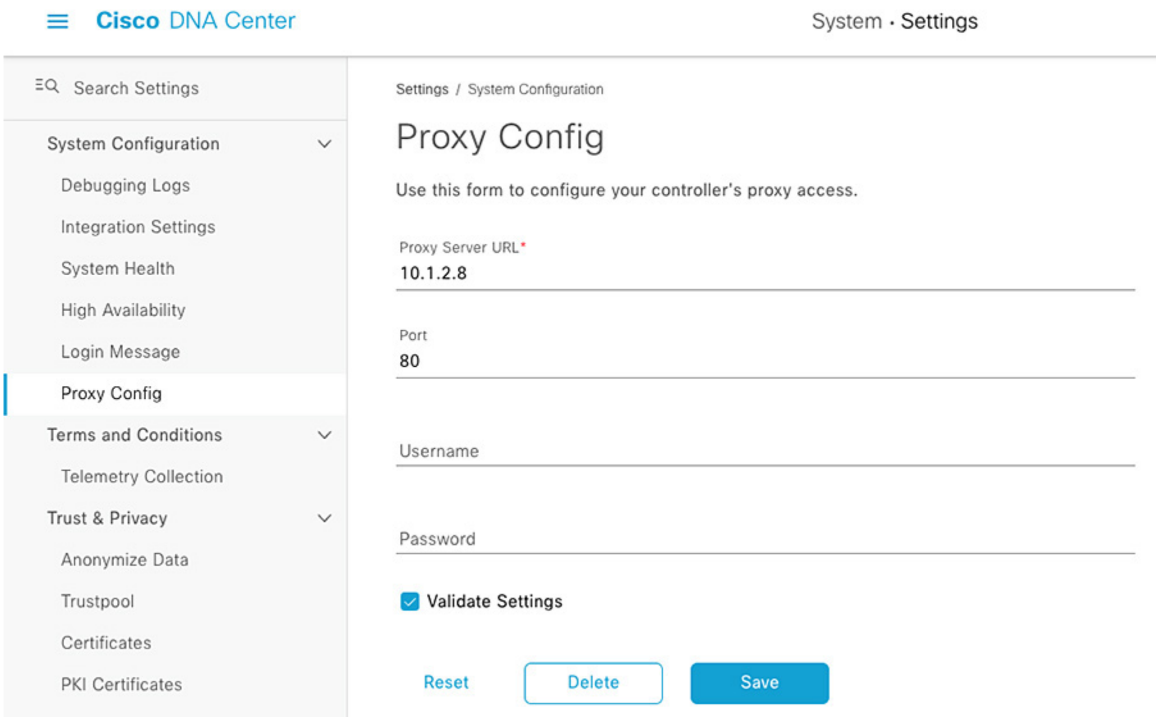
Client Id*: VJQFS-cfZ07Uk0ZuKzDXSqLFdQeRpGhNKnCyix33czad0j9_nywelSV3_UMemiP8

Client Secret*: ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••

## Proxy

In addition to using SSM for licensing, in this implementation we configured Cisco DNA Center to use a proxy for external web communication for tasks such as software image downloads. Proxy communication can be configured during Cisco DNA Center cluster installation or added later in **System > Settings > System Configuration >Proxy Config**.

**Figure 4 Cisco DNA Center Proxy Configuration**



Proxy Config

Use this form to configure your controller's proxy access.

Proxy Server URL* 10.1.2.8

Port 80

Username

Password

☑ Validate Settings

# Configuration

## Users and Roles

For this implementation, the default Cisco DNA Center users and roles were used:

- SUPER-ADMIN-ROLE—This role has full access within Cisco DNA Center to manage any devices, integrations, and Cisco DNA Center configuration.
- NETWORK-ADMIN-ROLE—This role can view and modify devices and configurations, but does not have privileges to make any changes to Cisco DNA Center itself.
- OBSERVER-ROLE—This role has read-only access to view non-sensitive information.

Navigate to **System > Users & Roles** to view or modify users and roles.

## Integrations

Cisco DNA Center integrates with Cisco ISE to establish unified environment tracking and control. To establish the communication between Cisco DNA Center and ISE, do the following:

1. From the Cisco DNA Center web interface, navigate to **System > Settings**.
2. From the Settings menu, choose **External Services > Authentication and Policy Servers**.
3. From the **Add** drop-down list, choose **ISE**.
   a. On the **Add ISE server** slide-in pane, in the **Server IP Address** field, enter the IP address of the ISE Primary Admin Node (PAN).

b. In the **Shared Secret** field, enter the secret for network access devices.

c. In the **Username** field, enter the ISE PAN administrator username.

d. In the **Password** field, enter the ISE PAN administrator password.

e. In the **FQDN** field, enter the fully-qualified domain name of the ISE PAN.

f. Click the **Add** button.

## Upgrade

Information for upgrading Cisco DNA Center can be found at: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/upgrade/b_cisco_dna_center_upgrade_guide.html.

**Note:** Cisco DNA Center availability is impacted while it is upgrading, however network devices and clients can continue to communicate normally with services such as ISE, DNS, and so on.

# Design

The Design feature set in Cisco DNA Center allows users to prepare the system to manage the intended infrastructure with the correct configurations and services. The process is as follows:

1. Create Sites
2. Define Network Settings
3. Confirm Image Repository
4. Define Templates
5. Configure Network Profile

## Sites

Cisco DNA Center allows users to logically organize managed systems into hierarchical Sites, which can be geographical or logical groups for ease of management and configuration consolidation. To create Sites, do the following:

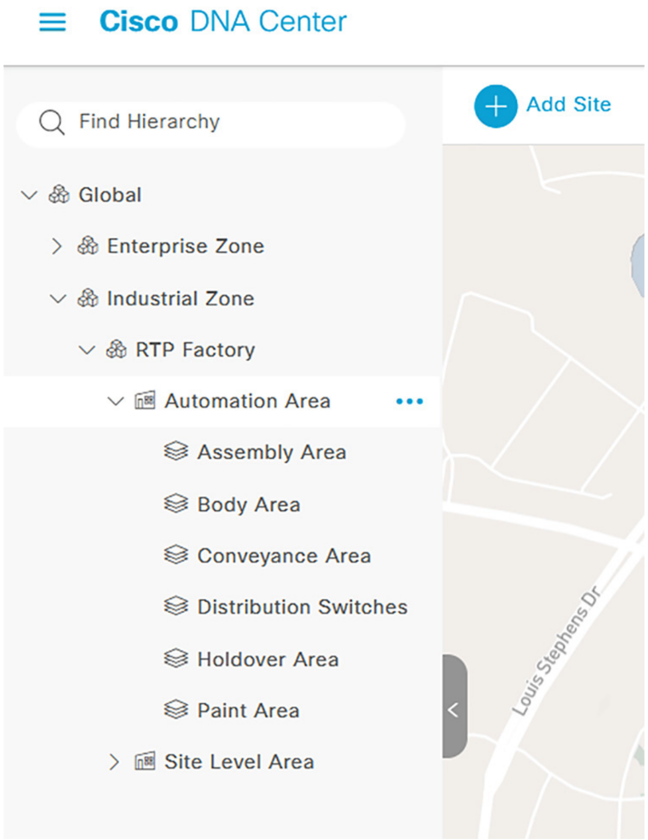
1. From the Cisco DNA Center web interface, navigate to **Design > Network Hierarchy**.
2. Click the **Add Site** button and select the appropriate option (for example, choose **Add Area** for a logical zone in the network).

   a. Enter the name and choose the immediate parent floor, building, or area.

   b. Click the **Add** button.

3. Repeat as needed to build the geographical or logical hierarchy suited to your environment.

**Figure 5 Cisco DNA Center Network Hierarchy**



**Note:** Moving devices between Sites will potentially initiate configuration changes; with Device Controllability enabled and Telemetry settings defined for each Site, moving a device to a new Site will trigger Cisco DNA Center to push configuration changes to align with the new Site settings. In addition, a Site cannot be deleted while it has devices assigned to it.

## Network Settings

Network Settings allow the user to tailor what Cisco DNA Center will configure by default on a per-Site basis, which helps simplify and streamline configuration. This guide will focus on Network and Telemetry settings as applicable to Industrial Automation switching. Network settings include services such as DHCP, DNS, NTP, AAA, and so on that the managed host will use for the respective network communications. Telemetry settings consist of SNMP Traps, Syslog, and NetFlow, which Cisco DNA center will use for monitoring device health and communication. To define Network Settings, do the following:

1. From the Cisco DNA Center web interface, navigate to **Design > Network Settings**.
2. On the **Network** tab, navigate to the desired Site from the left hierarchy.
    a. Click the **Add Servers** button.
    b. Check the checkbox next to each desired service. Click the **OK** button.
    c. For each Server chosen, enter the required information:
    – For **AAA Server**, check the **Network** and **Client/Endpoint** checkboxes to define the AAA server IP address and protocol to be used by the network device and any connected endpoints. In this implementation, the ISE PAN and RADIUS are used for both **Network** and **Client/Endpoint**. See note at the bottom of this section regarding AAA and RADIUS configuration.

- For **DHCP Server**, enter the IP address of the DHCP server.
- For **DNS Server**, enter the fully-qualified domain name in the **Domain Name** field and the DNS IP address in the **Primary** field.
- For **NTP Server**, enter the NTP server IP address in the **NTP** field.
- For **Time Zone**, choose the appropriate option from the **Time Zone** drop-down list.
- For **Message of the Day**, check the **Do not override the existing MOTD banner on the device** checkbox.
- Click the **Save** button.

d. Repeat for each Site accordingly.

3. On the Telemetry tab, navigate to the desired Site from the left hierarchy.

a. For **SNMP Traps**, check the **Use Cisco DNA Center as the SNMP trap server** checkbox.

b. For **Syslogs**, check the **Use Cisco DNA Center as syslog server** checkbox.

c. For **NetFlow**, you can check the **Use Cisco DNA Center as NetFlow collector server** or **Add an external NetFlow collector server** checkbox. We recommend to leave these unchecked and configure NetFlow using templates for the industrial network containing a majority of industrial switches.

d. For **Wired Client Data Collection**, check the **Monitor wired clients** checkbox. This feature enables IP Device Tracking (IPDT) on the device which tracks IP address to SGT bindings for endpoints to be used in TrustSec policy. See note at the bottom of this section regarding IPDT.

e. Click the **Save** button.

f. Repeat for each Site accordingly.

**Note:** Regarding AAA and RADIUS—As of release 2.2.3.3, Cisco DNA Center will apply all necessary configuration for AAA and RADIUS communication, however the following commands need to be added through a template for the IE3400 switch to have successful communication with ISE:

```
Switch(config)#cts authorization list dnac-cts-list
```

```
Switch(config-radius-server)#pac key 7 secret
```

**Note:** Regarding IPDT—For classic Cisco IOS platforms, the recommended option is to modify the standard IP address used with the IPDT feature prior to the implementation of IPDT. Using the default can cause the keepalive messages to be populated with duplicate IP addresses for the source and destination, potentially causing a communication issue for the connected end devices.

The following command can be added through a template:

```
Switch(config)#ip device tracking probe auto-source fallback 169.254.26.64 0.0.0.0 override
```

For more details see:
https://www.cisco.com/c/en/us/support/docs/ip/address-resolution-protocol-arp/118630-technote-ipdt-00.html.

**Note:** Not all Network Settings are applied simultaneously. Given that Device Controllability is enabled, Telemetry settings are applied when a device is assigned to a Site and the Network specific settings (AAA, DHCP, and so on) are applied when a device is provisioned.

## Image Repository

Cisco DNA Center communicates with Cisco.com to retrieve available software images for the suite of supported devices, whether directly or through a proxy. Similar to Network Settings, software versions can be specified on a per-Site basis to ensure consistent operation across devices. After devices have been discovered and added to Sites, you can change the Golden Image in Image Repository for each device type by doing the following:

1. From the Cisco DNA Center web interface, navigate to **Design > Image Repository**.
2. Choose the desired Site from the left hierarchy.
3. From the **Devices** list, expand each device to see all available software images. Click the **arrow** button in the **Golden Image** column to download the relevant image, and in the subsequent **Download Image** dialogue box, check the **Mark the image as golden after download** checkbox to set that image as the Golden Image for that specific device type.
4. Repeat for other devices and Sites as necessary.

## Templates

Cisco DNA Center Templates can be used to automate any configuration on discovered or managed devices, whether they are new or have existing configurations. See the Appendix for examples and tips on using templates. To create a template, do the following:

1. From the Cisco DNA Center web interface, navigate to **Tools > Template Editor**.
2. Click the **Plus** button and choose **Create Template**.

   a. Under **Template Type**, click the **Regular Template** radio button.

   b. Under **Template Language**, click the **Velocity** radio button. The **Jinja** option can be used as well; for more details refer to Cisco DNA Center Documentation: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3.html.

   c. Under **Name**, enter a name for the template.

   d. From the **Project Name** drop-down list, choose the relevant project. For example, choose **Onboarding Configuration** to create a template to be used for initial configuration of a new device during Plug and Play.

   – Click the **Edit** link under **Device Type(s)**.

   – Navigate through the expandable lists to check the boxes for all relevant devices.

   e. At the top, click the **Back to Add New Template** link.

   f. From the **Software Type** drop-down list, choose the appropriate Cisco software type.

   g. Click the **Add** button.

   h. The **Template Editor** pane will display, allowing you to enter CLI commands for configuration. Note that variables may be used by denoting a dollar sign with the argument; for example:

```
ip address $address 255.255.255.0
```

   i. After adding all desired configuration, from the **Actions** drop-down list choose **Save** and then choose **Commit**.

**Note:** Any changes to existing templates do not trigger a configuration change on associated devices until they are provisioned again.

## Network Profiles

Cisco DNA Center Network Profiles allow you to attach templates to Sites so that when a device is added to the Site, Cisco DNA Center will automatically apply the configuration specified in the template. To create a Network Profile, do the following:

1. From the Cisco DNA Center web interface, navigate to **Design > Network Profiles**.
2. From the **Add Profile** drop-down list, choose the appropriate device type.
   a. For the **Profile Name** field, enter a name.
   b. Choose the **OnBoarding Template(s)** tab to attach any templates to be used during Plug and Play for unconfigured devices or the **Day-N Template(s)** tab to attach any templates for additional configuration to be pushed during provisioning.
   c. Click the **Add Template** button.
   - On the **Add Template** slide-in pane, choose the relevant template from the **Templates** list.
   - Click the **Add** button.

   d. Click the **Save** button.

**Note:** Adding a template to a Network Profile will not trigger a configuration change on applicable existing devices until they are provisioned again.

# Automation

The automation features in Cisco DNA Center provide a powerful toolset for monitoring and managing your infrastructure. This helps with maintaining inventory, ensuring consistent configuration, and driving compliance. The process is as follows:

1. Manage devices with Discovery or Plug and Play
2. Monitor with Topology and Inventory
3. Maintain devices SWIM and RMA workflows

There are three main workflows in Industrial Automation networks for adding devices to Cisco DNA Center–Discovery, Plug and Play, and Offline provisioning. In the following sections we give details about the Discovery and Plug and Play methods and discuss some of the variety of Inventory features that can used to manage these devices.

**Note:** For Offline provisioning we use Cisco DNA Center Discovery; the device is configured manually via CLI or other management tools and is then discovered by Cisco DNA Center when network connectivity is established. See the Appendix for further details.

## Discovery

Cisco DNA Center can discover network devices and add them to the managed inventory, which can help administrators maintain and monitor the environment from a central viewpoint. The Device Controllability feature can be added to the discovery process to prepare devices for management through Cisco DNA Center when subsequent provisioning configuration or inventory changes are made. To discover devices, do the following:

1. From the Cisco DNA Center web interface, navigate to **Tools > Discovery**.
2. Click the **Add Discovery** button.

a. Note at the bottom if Device Controllability is enabled (it is enabled by default). If enabled, Cisco DNA Center will configure SNMP or NETCONF credentials on the device during Discovery (it will not overwrite existing SNMP or NETCONF configuration). We recommend using Device Controllability to make use of the Cisco DNA Center monitoring capabilities.

   **Note:** Currently Cisco IE switches can be discovered via NETCONF however there are no additional capabilities from it in the current release. If you do not want any configuration changes made to the device(s), click the **Disable** link.

b. In the **Discovery Name** field, enter a name for the relevant device(s) being discovered.

c. Under **IP Address/Range**, choose the appropriate **Discovery Type**:

– For **CDP**, enter the **IP Address** of a device to be discovered. You can change the **CDP Level** to something other than the default to detect more or fewer neighboring devices to the original device.

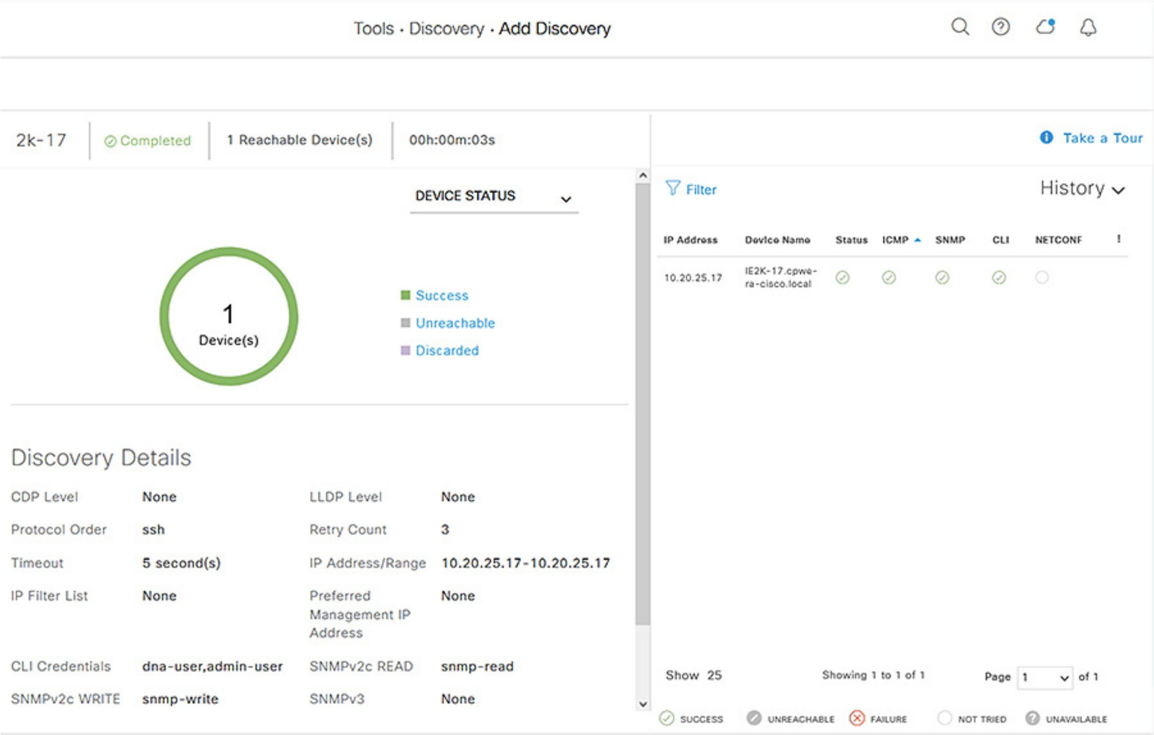
– For **IP Address/Range**, in the **From** field enter the lowest IP address to be scanned. In the **To** field, enter the highest IP address to be scanned. If only one device is being discovered, enter the same IP address in both fields. The IP address method is recommended for discovering devices.

– For **LLDP**, enter the **IP Address** of a device to be discovered. You can change the **LLDP Level** to something other than the default to detect more or fewer neighboring devices to the original device.

d. Under **Credentials**, click the toggle buttons of the necessary entities under **CLI, SNMPv2c Read, SNMPv2c Write**, and so on. The device being discovered must accept at least one form of these credentials for discovery to be successful and CLI credentials are mandatory.

e. Click the **Discover** button. The Discovery process will begin and show progress on the Discovery page with automatic refreshing to display the current status. When the process is finished, it will display success or failure results and add the discovered device to Inventory.

**Figure 6 Cisco DNA Center Discovery**



2k-17 | ✓ Completed | 1 Reachable Device(s) | 00h:00m:03s

| IP Address | Device Name | Status | ICMP | SNMP | CLI | NETCONF |
|---|---|---|---|---|---|---|
| 10.20.25.17 | IE2K-17.cpwe-ra-cisco.local | ✓ | ✓ | ✓ | ✓ | ○ |

Show 25 Showing 1 to 1 of 1 Page 1 of 1

Discovery Details

| | | | |
|---|---|---|---|
| CDP Level | None | LLDP Level | None |
| Protocol Order | ssh | Retry Count | 3 |
| Timeout | 5 second(s) | IP Address/Range | 10.20.25.17-10.20.25.17 |
| IP Filter List | None | Preferred Management IP Address | None |
| CLI Credentials | dna-user,admin-user | SNMPv2c READ | snmp-read |
| SNMPv2c WRITE | snmp-write | SNMPv3 | None |

After discovery, you can assign the device to a Site and Provision, which can be done individually or in the same step.

Assign to Site only:

1. Navigate to **Provision > Network Devices > Inventory**.
2. From the left Hierarchy, choose **Global > Unassigned Devices**.
3. Locate the newly discovered device in the list and check the checkbox. From the **Actions** drop-down list, choose **Provision > Assign Device to Site**.
    a. On the **Assign Device to Site** slide-in pane, click the **Choose a Site** link. Click the desired site from the hierarchy then click the **Save** button. Click the **Next** button.

    b. Review the settings that will be deployed, then click the **Next** button.

    c. Click the **Now** radio button to make the change immediately (if scheduling the assignment for a future date and time, click the **Later** radio button and specify the date and time).

    d. Click the **Assign** button.

After the device has been assigned, it will be in the device list of the specified Site. Note that when Device Controllability is enabled, assigning the device to a Site will trigger the following configurations (where applicable):

- Controller certificates
- SNMP trap server definitions
- Syslog server definitions
- NetFlow server definitions
- IPDT enablement

Assign to Site and Provision:

1. Navigate to **Provision > Network Devices > Inventory**.
2. From the left Hierarchy, choose **Global > Unassigned Devices**.
3. Locate the newly discovered device in the list and check the checkbox. From the **Actions** drop-down list, choose **Provision > Provision device**.
    a. On the **Assign Site** step, click the **Choose a site** link and choose the desired Site. Click the **Save** button, then click the **Next** button. (Note that if Site assignment was done previously no action is needed here).

    b. On the **Advanced Configuration** step, choose the device from the **Devices** list if there are any template settings to be configured. When finished, or if no template is applied, click the **Next** button.

    c. On the **Summary** step, review the configuration to be added to the device. Click the **Deploy** button.

After the device has been provisioned, it will be in the device list of the specified Site.

**Note:** For Cisco DNA Center release 2.2.3.3:

- Provisioning a device that has been already been configured with AAA before being discovered will fail. Remove any AAA configuration before pushing AAA using Cisco DNA Center.
- There is a known defect in which AAA provisioning fails for the Cisco IE 2000 switch and subsequent provisioning tasks are aborted.

# Plug and Play

One of the most powerful tools of Cisco DNA Center is Plug and Play (PnP). You can prepare for new, unconfigured devices in advance or detect them on the network in real time, and Cisco DNA Center can claim and configure these devices without user interaction on the device itself. The process is as follows:

1. Connect the new device to the network. See the Appendix for notes on PnP network preparation.
2. From the Cisco DNA Center web interface, navigate to **Provision > Network Devices > Plug and Play**.
3. The **Plug and Play** page will show any currently Unclaimed devices. These can be claimed and added to Inventory. For preparing for future devices to be claimed, skip to Step 5.
4. Check the checkbox for all devices being claimed and from the **Actions** drop-down list choose **Claim**.
   a. On the **Assign Site** step, under the **Site** column, click the **Assign** link. Choose the appropriate Site and click the **Assign** button. Repeat for any other devices or check the **Apply Site to All** checkbox to configure them all for the same Site. Click the **Next** button.

   b. On the **Assign Configuration** step, a software image and template can be chosen to apply to the device when it is claimed. The template is automatically chosen based on the Onboarding templates for the given device type at the given Site. Click the software image or template link to show the **Configuration** slide-in pane, where the image can be changed or removed (if no software image change is desired). Note that if the image is being changed, the device will reload during the PnP process. The template can also be changed or removed. When the desired image and template are selected (or removed), click the **Save** button. Then click the **Next** button.

   c. On the **Provision Templates** step, choose the device from the **Devices** list and enter any required information as specified in the template (the values for each template variable). Repeat for all devices. Click the **Next** button.

   d. On the **Summary** step, review the configuration and details. Click the **Claim** button to begin the claiming process, which will make configuration changes on the device and add it to Inventory.
5. To prepare Cisco DNA Center to claim devices not yet connected to the network in advance, from the **Plug and Play** page click the **Add Devices** button.
6. On the **Add Devices** slide-in pane, choose the appropriate method:
   - **Single Device**–Enter the **Serial Number**, **Product ID**, and optional **Device Name**. Click the **Add Device** button (you will claim it manually as previously discussed once it is detected by Cisco DNA Center) or the **Add+Claim** button (the claim is configured now).
   - **Bulk Devices**–Click the **Download File Template** button to download a .CSV file template, which instructs on how to specify multiple devices at once. Upload the file and click the **Import Devices** button.
   - **Smart Account Devices**–For further details see the Cisco DNA Center User Guide: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_01101.html#id_89077.

After the devices have been claimed, they can be provisioned by following Steps 3-5 in the Discovery section.

# Topology

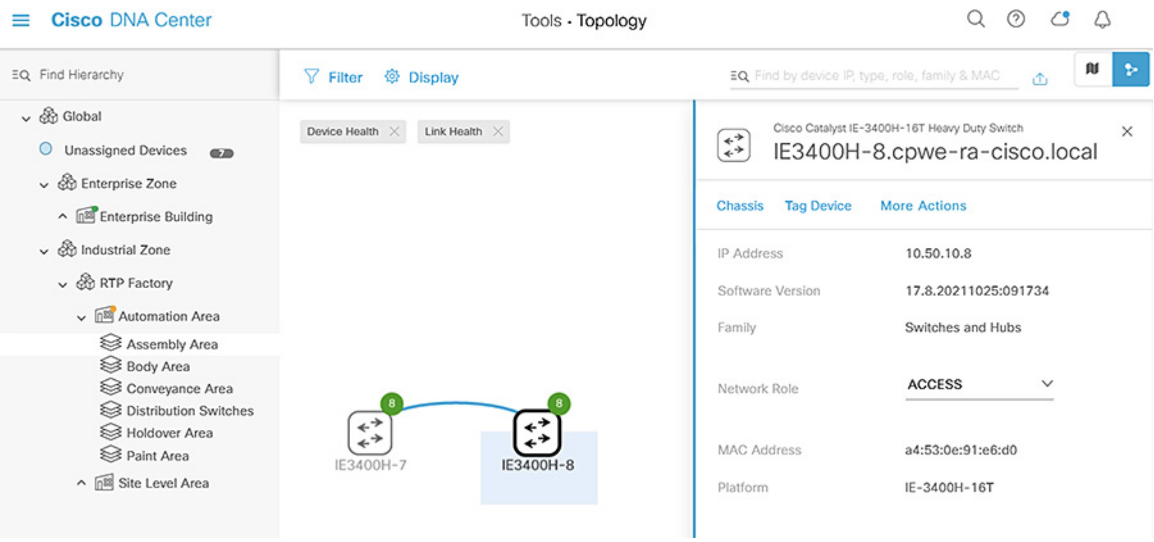
The Topology view in Cisco DNA Center is a useful tool for visualizing the network because it shows devices and their connections as well as device and link details, giving administrators a better understanding of the network and its health. To view the Topology, do the following:

1. From the Cisco DNA Center web interface, navigate to **Tools > Topology**.
2. From the left Hierarchy, choose a Site to view the respective devices and links.

From the Topology view you can:

- Hover over a link to view the speed or click on a link to view the connection details.
- Hover over a device to view the device type and network details or click on the device to view additional details and navigate to other Cisco DNA Center menus for the given device.
- Filter what is shown based on specific network criteria. Click the **Filter** button at the top and choose **VRF, VLAN, Routing**, or **Tagging**. This will narrow the scope of what is displayed to only devices and connections that meet the specified network criteria.

**Figure 7 Cisco DNA Center Topology**



Cisco Catalyst IE-3400H-16T Heavy Duty Switch

IE3400H-8.cpwe-ra-cisco.local

IP Address 10.50.10.8

Software Version 17.8.20211025:091734

Family Switches and Hubs

Network Role ACCESS

MAC Address a4:53:0e:91:e6:d0

Platform IE-3400H-16T

# Inventory

Cisco DNA Center Inventory has a wide variety of capabilities to manage devices. Once a device has been discovered or added to inventory through PnP, it can be provisioned, which adds the specified Network Settings to devices. In addition, after devices are fully managed, Inventory can provide compliance and software verification, as well as options to change device settings or initiate device replacement. The following section details some of the monitoring and management capabilities in Inventory.

## Software Image Management

Devices can be upgraded automatically through Cisco DNA Center, which downloads the image from Cisco.com, pushes the image to the device, and performs the upgrade. In addition, you have the option of uploading a desired image to Cisco DNA Center and upgrades can be scheduled in advance . After ensuring the image is set as Golden (see the Image Repository section), update a device's software image by doing the following:

1. From the Cisco DNA Center web interface, navigate to **Provision > Network Devices > Inventory**.
2. From the left Hierarchy, choose the Site with the device to be upgraded.
3. Check the checkbox next to the device to be upgraded and from the **Actions** drop-down list choose **Software Image > Update Image**.
4. From the **Image Upgrade** slide-in pane, check the checkbox of the device to be upgraded and click the **Next** button.

5. Under **Software Distribution**, click the **Now** radio button (if scheduling an upgrade for a future date and time, click the **Later** radio button and specify the date and time). Click the **Next** button.

6. Under **Software Activation**, check the **Initiate Image Activation after Image Distribution is finished** checkbox. If you just want to push the image to the device and not launch the upgrade, leave the box unchecked and either specify the start date and time or click the **Skip Activation** link at the bottom. You also have the option of checking the **Initiate Flash Cleanup after Activation** checkbox, which will automatically remove unused software image files from the device after the upgrade. Click the **Next** button.

7. On the **Summary** step, review the upgrade details and then click the **Submit** button.

### Notes on software image management:

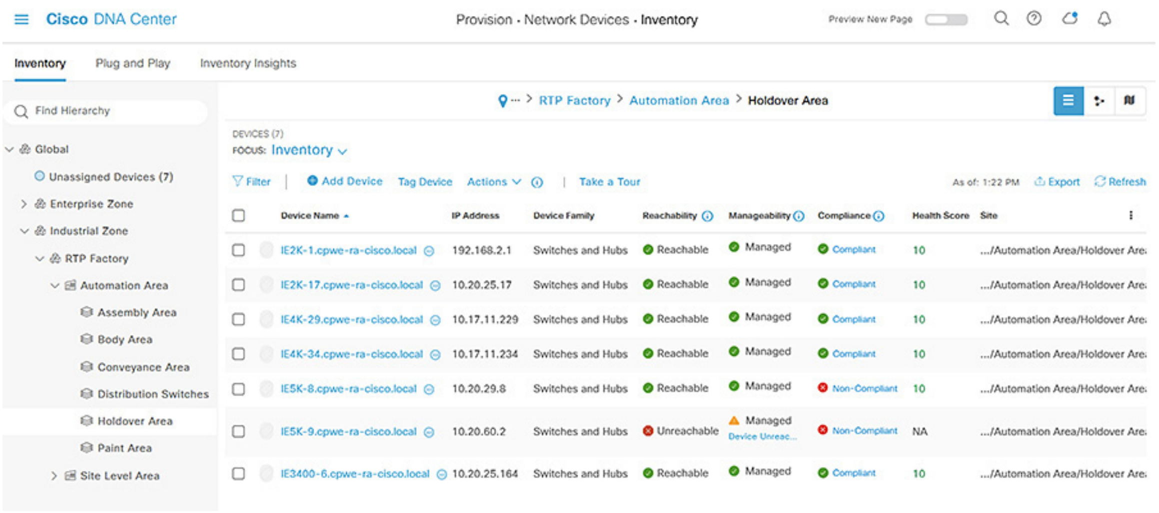
- Cisco DNA Center will give priority to installing and running the image on sdflash if it is present. If the software is running in Install mode from flash with sdflash present, the upgrade will fail.

- If the image is running on sdflash and it is formatted as vfat the upgrade will be successful. If it is formatted in ext4 only (for Cisco Cyber Vision) the upgrade will fail. See IOS XE Devices with Cisco Cyber Vision for details on partitioning sdflash, which allows the software image and iox applications to run concurrently from sdflash.

- The update process will trigger a reload on the device which will impact network connectivity for the device and any connected endpoints.

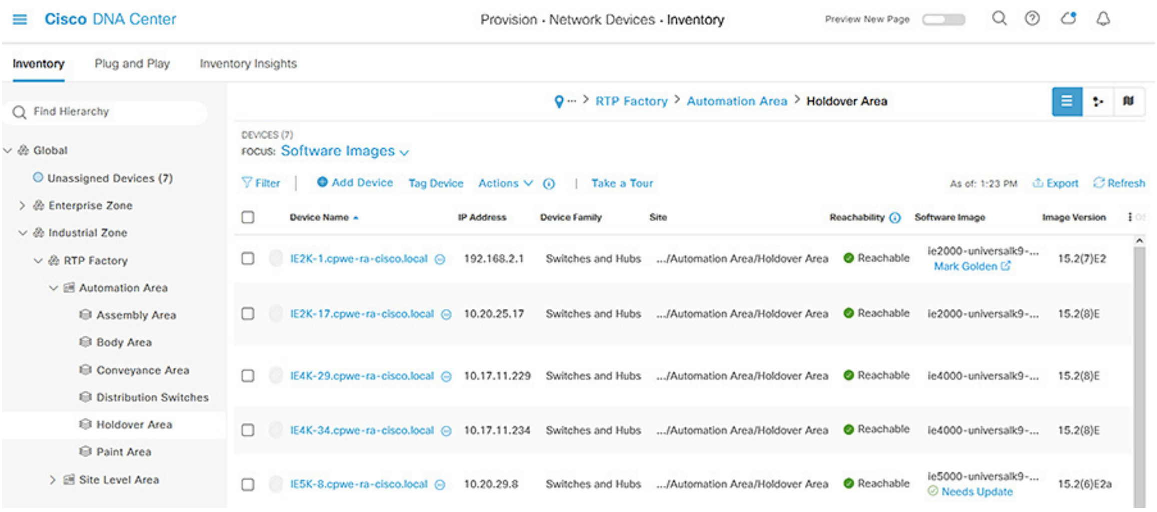
On the **Inventory** page, you can review the status of the update by choosing **Software Image > Image Update Status** from the **Actions** drop-down list. In addition, from **Inventory** you can review which devices are not running the specified Golden Image with the **Compliance** status column or choosing **Software Images** from the **Focus** drop-down list.

**Figure 8 Cisco DNA Center Inventory**



| □ | Device Name | IP Address | Device Family | Reachability | Manageability | Compliance | Health Score | Site |
|---|---|---|---|---|---|---|---|---|
| □ | IE2K-1.cpwe-ra-cisco.local | 192.168.2.1 | Switches and Hubs | Reachable | Managed | Compliant | 10 | .../Automation Area/Holdover Are: |
| □ | IE2K-17.cpwe-ra-cisco.local | 10.20.25.17 | Switches and Hubs | Reachable | Managed | Compliant | 10 | .../Automation Area/Holdover Are: |
| □ | IE4K-29.cpwe-ra-cisco.local | 10.17.11.229 | Switches and Hubs | Reachable | Managed | Compliant | 10 | .../Automation Area/Holdover Are: |
| □ | IE4K-34.cpwe-ra-cisco.local | 10.17.11.234 | Switches and Hubs | Reachable | Managed | Compliant | 10 | .../Automation Area/Holdover Are: |
| □ | IE5K-8.cpwe-ra-cisco.local | 10.20.29.8 | Switches and Hubs | Reachable | Managed | Non-Compliant | 10 | .../Automation Area/Holdover Are: |
| □ | IE5K-9.cpwe-ra-cisco.local | 10.20.60.2 | Switches and Hubs | Unreachable | Managed<br>Device Unreac... | Non-Compliant | NA | .../Automation Area/Holdover Are: |
| □ | IE3400-6.cpwe-ra-cisco.local | 10.20.25.164 | Switches and Hubs | Reachable | Managed | Compliant | 10 | .../Automation Area/Holdover Are: |

**Figure 9 Cisco DNA Center Inventory–Software Images**



| Device Name | IP Address | Device Family | Site | Reachability | Software Image | Image Version |
|---|---|---|---|---|---|---|
| IE2K-1.cpwe-ra-cisco.local | 192.168.2.1 | Switches and Hubs | .../Automation Area/Holdover Area | Reachable | ie2000-universalk9-...<br>Mark Golden | 15.2(7)E2 |
| IE2K-17.cpwe-ra-cisco.local | 10.20.25.17 | Switches and Hubs | .../Automation Area/Holdover Area | Reachable | ie2000-universalk9-... | 15.2(8)E |
| IE4K-29.cpwe-ra-cisco.local | 10.17.11.229 | Switches and Hubs | .../Automation Area/Holdover Area | Reachable | ie4000-universalk9-... | 15.2(8)E |
| IE4K-34.cpwe-ra-cisco.local | 10.17.11.234 | Switches and Hubs | .../Automation Area/Holdover Area | Reachable | ie4000-universalk9-... | 15.2(8)E |
| IE5K-8.cpwe-ra-cisco.local | 10.20.29.8 | Switches and Hubs | .../Automation Area/Holdover Area | Reachable | ie5000-universalk9-...<br>Needs Update | 15.2(6)E2a |

## IOS XE Devices with Cisco Cyber Vision

Cisco DNA Center will store and run the software image on SD flash if it is present on the device, therefore special preparation must be done for IOS XE devices that will be running Cisco Cyber Vision Sensor (Cisco IE 3400 requires a minimum software release of 17.5 and Cisco IE 3400H requires a minimum software release of 17.7). To prepare the device, do the following:

1. Set the boot variable to run the software image from flash if it is not already.

```
Switch(config)#boot system flash:filename
```

2. Stop IOX if it is running and format SD flash to vfat. Note that if Cyber Vision Sensor is already installed, this step will remove it.

```
Switch(config)#no iox
Switch(config)#exit
Switch#format sdflash:
```

3. Save the configuration.

```
Switch#copy running-config startup-config
```

4. Partition SD flash to allocate 73% of the storage space to IOX. After partitioning, the switch will reload.

```
Switch#partition sdflash: iox 73
```

5. When the switch is available, verify the partitioning.

```
Switch#show sdflash: filesystem
Filesystem: sdflash
Filesystem Path: /flash12
Filesystem Type: vfat
Mounted: Read/Write

IOx Partition Exists
IOx Partition Type: ext4
IOx Partition Path: /flash11
IOx Partition Size: 2.7 G
IOS Partition Size: 1.2 G
```

6. Run the **sync** command to transfer files from flash: to sdflash.

   ```
   Switch#sync flash: sdflash:
   ```

7. Update the boot variable to run from sdflash.

   ```
   Switch(config)#no boot system flash:filename
   Switch(config)#no boot flash-primary
   Switch(config)#boot system sdflash:filename
   ```

8. Save the configuration.

   ```
   Switch#copy running-config startup-config
   ```

9. Reload the switch.

   ```
   Switch#reload
   ```

10. When the switch is available, start IOX.

   ```
   Switch(config)#iox
   ```

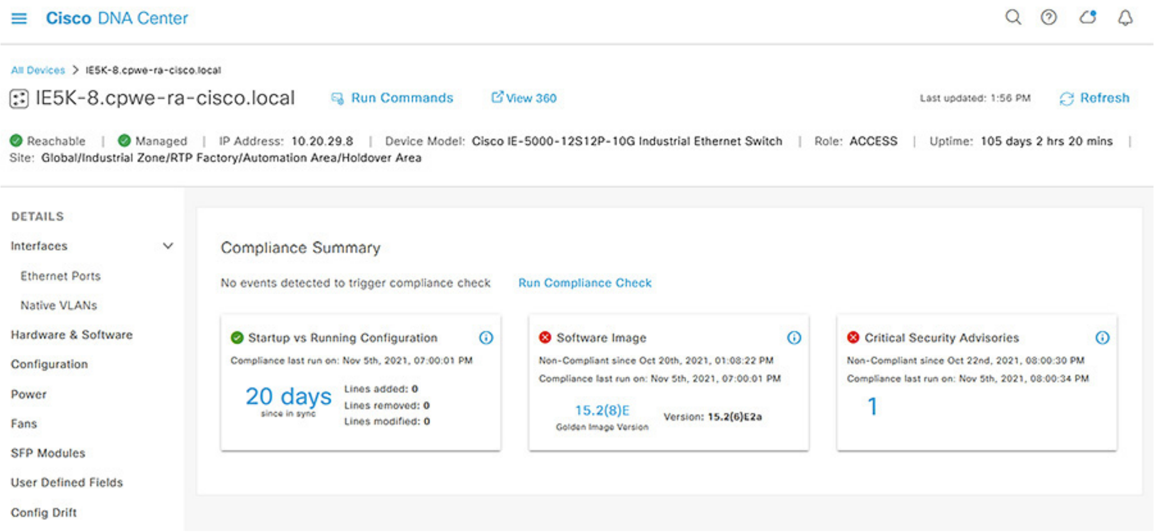
The device is now able to be upgraded through Cisco DNA Center as well as run Cisco Cyber Vision Sensor. Note that the above configuration can be included in a Day-N template, however be sure that the necessary boot image and SD flash are present on the device.

## Device Compliance

Cisco DNA Center Compliance monitors devices for software image, configuration drift, and potential security issues based on the software image, giving administrators an up-to-date status of device posture. To view the compliance information for a given device, do the following:

1. From the Cisco DNA Center web interface, navigate to **Provision > Network Devices > Inventory**.
2. From the left Hierarchy, choose the Site with the device to be upgraded.
3. For a given device, click the link under the **Compliance** column to view the status. For non-compliant devices, Cisco DNA Center will give details on the configuration or image issues to aid in remediation.

**Figure 10 Cisco DNA Center Compliance**



IE5K-8.cpwe-ra-cisco.local

Last updated: 1:56 PM

Reachable | Managed | IP Address: 10.20.29.8 | Device Model: Cisco IE-5000-12S12P-10G Industrial Ethernet Switch | Role: ACCESS | Uptime: 105 days 2 hrs 20 mins |
Site: Global/Industrial Zone/RTP Factory/Automation Area/Holdover Area

Compliance Summary

No events detected to trigger compliance check

Startup vs Running Configuration
Compliance last run on: Nov 5th, 2021, 07:00:01 PM
20 days since in sync
Lines added: 0
Lines removed: 0
Lines modified: 0

Software Image
Non-Compliant since Oct 20th, 2021, 01:08:22 PM
Compliance last run on: Nov 5th, 2021, 07:00:01 PM
15.2(8)E Golden Image Version
Version: 15.2(6)E2a

Critical Security Advisories
Non-Compliant since Oct 22nd, 2021, 08:00:30 PM
Compliance last run on: Nov 5th, 2021, 08:00:34 PM
1

Clicking on the compliance issue in question will provide further details. If **Software image** or **Critical Security Advisories** are out of compliance, typically a software upgrade will address the issue and can be initiated through Inventory. If **Startup vs Running Configuration** is out of compliance, you have the option to click the **Sync Device Config** from the details page.

## Device Replacement Workflow

In the event that a device is in need of replacement, Cisco DNA Center Inventory will allow you to mark the device for replacement in preparation for the Replace Device workflow. Cisco DNA Center will automatically configure a DHCP server on a neighboring device to aid the process of replacement. To mark a faulty device for replacement, do the following:

1. From the Cisco DNA Center web interface, navigate to **Provision > Network Devices > Inventory**.
2. From the left Hierarchy, choose the Site with the device to be upgraded.
3. Check the checkbox next to the device to be upgraded and from the **Actions** drop-down list choose **Device Replacement > Mark for Replacement**.
4. Click the **Mark** button.

The Replace Device workflow automatically provisions the new device with the last retrieved full configuration of the faulty device as well as adding the new device to Inventory. In addition, the workflow will update the software image to that of the faulty device (which will cause a momentary communication disruption on the new device). The new device being used for replacement must have the exact same product ID as the faulty device and the uplink interface should be the same to avoid communication disruption. The process is as follows:

1. Connect the new device to the network and allow the Cisco DNA Center PnP process to discover the device (no need to claim the device). See the Appendix for notes on PnP network preparation.
2. From the Cisco DNA Center web interface, navigate to **Workflows**.
3. Click the **Replace Device** button, then click the **Let's Do it** button.
4. On the **Choose Device Type** page, click the appropriate radio button for the device being replaced, then click the **Next** button.
5. On the **Choose Site** page, choose the appropriate Site from the hierarchy for the faulty device, then click the **Next** button.
6. On the **Choose Faulty Device** page, click the radio button of the faulty device, then click the **Next** button.
7. Under **Available Replacement Devices**, click the radio button of the new device, then click the **Next** button.
8. On the **Schedule Replacement** page, click the **Now** radio button (if scheduling the replacement for a future date and time, click the **Later** radio button and specify the date and time). Click the **Next** button.
9. On the **Summary** page, review the details. Click the **Replace** button.

**Note:** As of Cisco DNA Center release 2.2.3.3, there is an issue with upgrading devices during the remediation process if they are currently running a .tar software image (instead of .bin).

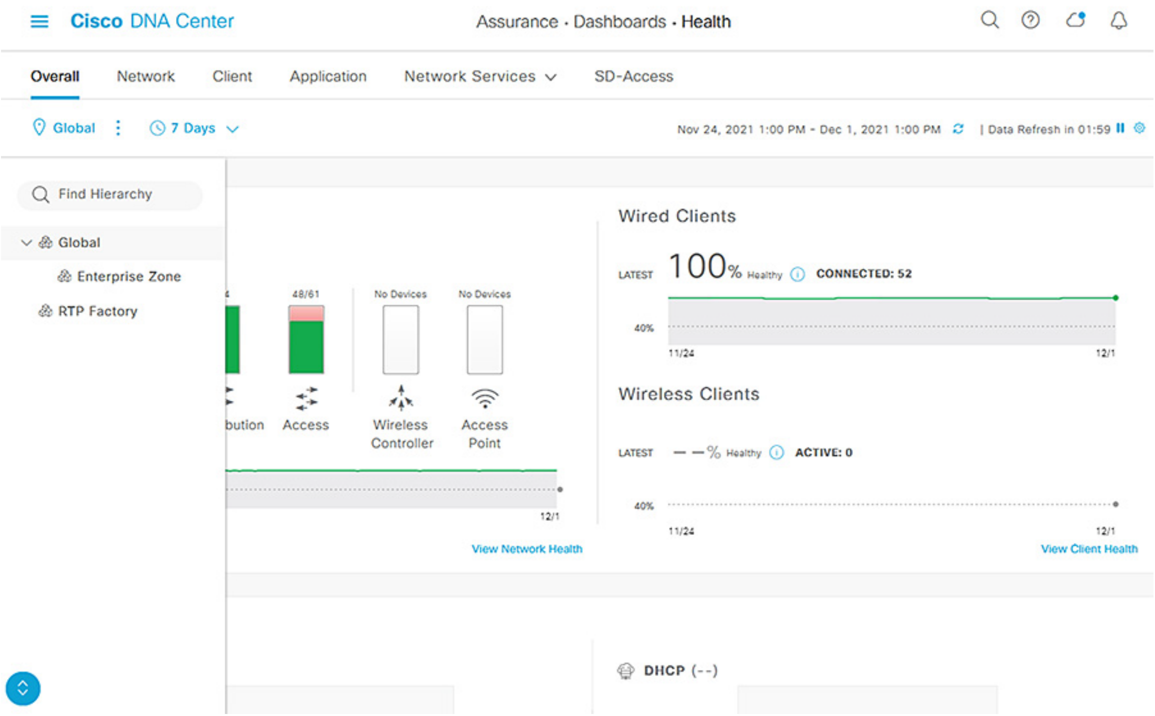
# Assurance

## Overview

Cisco DNA Assurance provides a wealth of information to monitor the status and health of devices and endpoints. The telemetry data is collected in intervals after assigning a device to a Site and the device will send SNMP traps to Cisco DNA Center as events occur. Note that primarily only syslog levels of Emergency, Alert, and Critical are sent by default (see https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/2-2-3/b_cisco_dna_assurance_2_2_3_ug/b_cisco_dna_assurance_2_2_2_ug_chapter_0110.html?bookSearch=true#reference_rxn_ntr_rgb). The Assurance health dashboard on the Cisco DNA Center web interface (**Assurance > Dashboard > Health**) gives an overview of issues and device health.

**Note:** The Health Dashboard displays the Global Site by default. The scope of the information displayed can be changed to Area or Building by clicking the **Global** link.

**Figure 11 Cisco DNA Center Health Dashboard**



## Network and Client Health Status

Cisco DNA Center gives distinct consideration to network device and client monitoring. Under **Assurance > Dashboards > Health > Network**, you can see an overview of all managed devices and on the **Network Devices** pane, you can filter the list to view details for a specific device.Click the link in the **Device Name** column to open the Device 360 details of that device. The **Device 360** page gives time-based details about the device health, including:

- **Device Details**–Model, IP address, uptime, software version, and so on
- **Issues**–Cisco DNA Center has a standardized list of issues of varying priority, which can be tuned to meet the needs of your environment. Issues are generated from telemetry data.

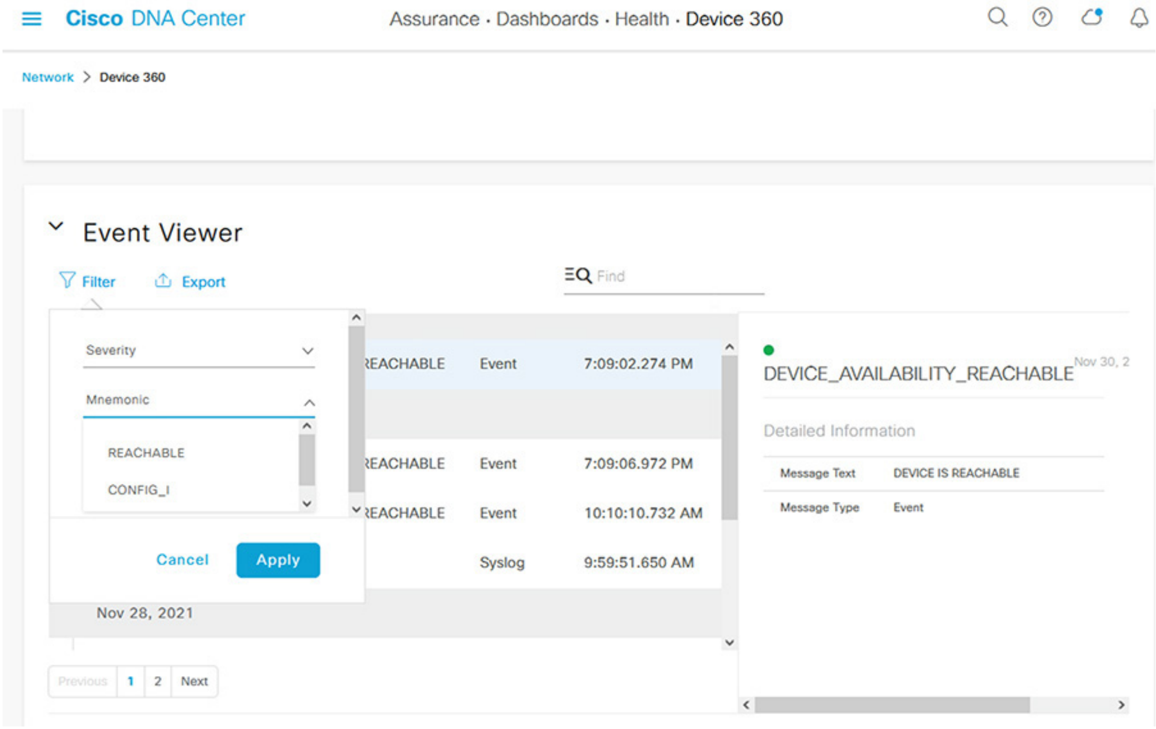
- **Physical Neighbor Topology**–A miniature topology view of the device showing connection(s) to other device(s), highlighting link and device health in the graphic
- **Event Viewer**–SNMP trap messages sent from the device to Cisco DNA Center

For clients, navigate to **Assurance > Dashboards > Health > Client** to view the Client 360 dashboard. Similar to network devices, Cisco DNA Center highlights issues and health of endpoints over time. On the **Client Devices** pane, click the link in the **Identifier** column to open the **Client 360** page for the endpoint. The **Client 360** page gives time-based details about endpoint health, including:

- **Client Details**–MAC address, IP address, connection status, and so on.
- **Issues**–The client issues stem from the associated network device for the endpoint but are specific to the health of the endpoint communications.
- **Onboarding**–A graphic displaying the endpoint and network device connection health
- **Event Viewer**–SNMP trap messages sent from the network device to Cisco DNA Center
- **Path Trace**–This feature is particularly useful in troubleshooting communication between the endpoint and another entity on the network. It checks the network between the two entities to determine if there is any cause for disruption.

The time frame of the Device and Client 360 information can be changed to give administrators a historical look back at events. Click the clock link at the top left of the Device 360 or Client 360 page to adjust the time setting. To change Issue thresholds to suit your environment, navigate to **Assurance > Manage > Issue Settings**. In addition, the **Event Viewer** also has a **Filter** link to narrow down the events displayed for network devices or clients.

**Figure 12 Cisco DNA Center Assurance Event Viewer**



| | | |
|---|---|---|
| REACHABLE | Event | 7:09:02.274 PM |
| REACHABLE | Event | 7:09:06.972 PM |
| REACHABLE | Event | 10:10:10.732 AM |
| | Syslog | 9:59:51.650 AM |

Nov 28, 2021

DEVICE_AVAILABILITY_REACHABLE Nov 30, 2

Detailed Information

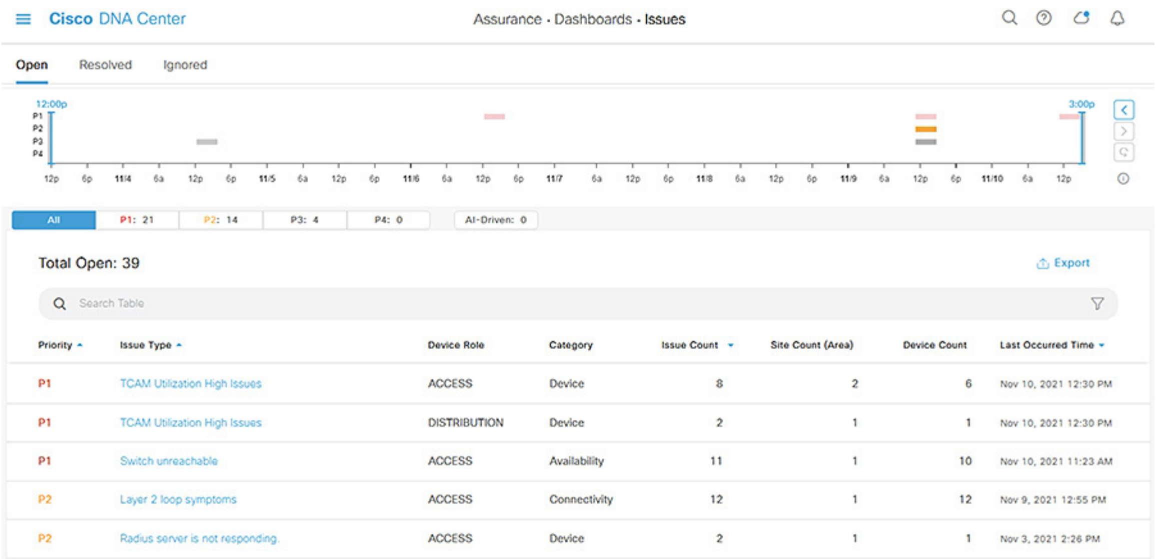
| | |
|---|---|
| Message Text | DEVICE IS REACHABLE |
| Message Type | Event |

# Issue Troubleshooting Example

A consolidated list of issues can be found at **Assurance > Dashboards > Issues** and by navigating through the Issues pages Cisco DNA Center can help provide root cause analysis. Here is an example of using Cisco DNA Center Issues to troubleshoot a device problem.

1. From the **Assurance > Dashboards > Issues** page, click the **Layer 2 loop symptoms** link under the **Issue Type** column.

**Figure 13 Cisco DNA Center Issues Dashboard**

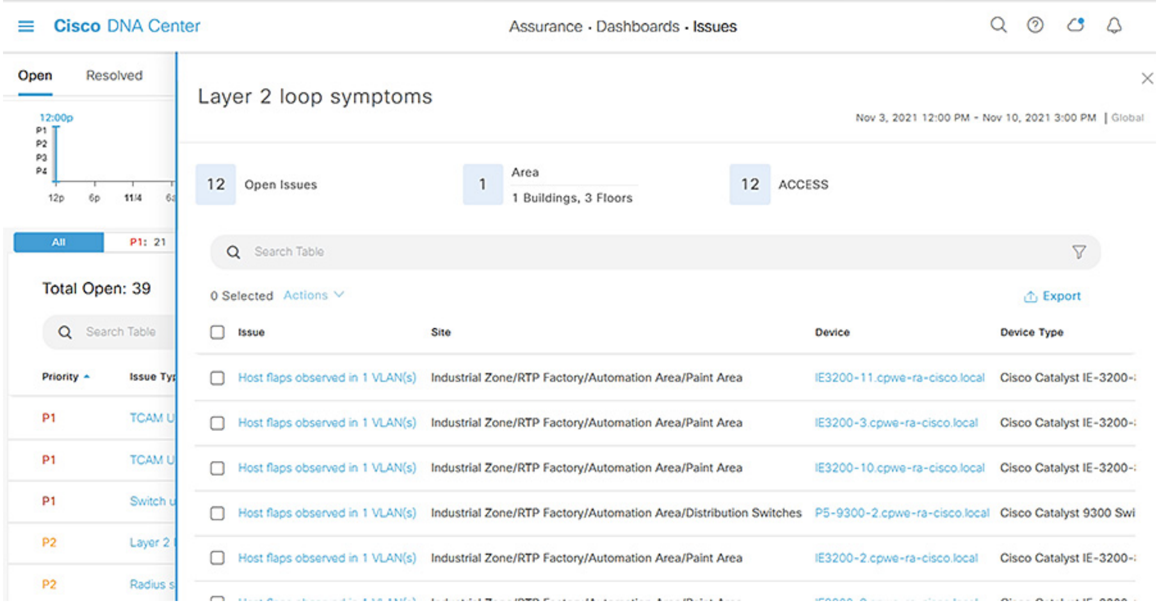

Cisco DNA Center
Assurance · Dashboards · Issues
Open
Resolved
Ignored
12:00p
3:00p
P1
P2
P3
P4
12p 6p 11/4 6a 12p 6p 11/5 6a 12p 6p 11/6 6a 12p 6p 11/7 6a 12p 6p 11/8 6a 12p 6p 11/9 6a 12p 6p 11/10 6a 12p
All
P1: 21
P2: 14
P3: 4
P4: 0
AI-Driven: 0
Export
Search Table

Total Open: 39

| Priority | Issue Type | Device Role | Category | Issue Count | Site Count (Area) | Device Count | Last Occurred Time |
|---|---|---|---|---|---|---|---|
| P1 | TCAM Utilization High Issues | ACCESS | Device | 8 | 2 | 6 | Nov 10, 2021 12:30 PM |
| P1 | TCAM Utilization High Issues | DISTRIBUTION | Device | 2 | 1 | 1 | Nov 10, 2021 12:30 PM |
| P1 | Switch unreachable | ACCESS | Availability | 11 | 1 | 10 | Nov 10, 2021 11:23 AM |
| P2 | Layer 2 loop symptoms | ACCESS | Connectivity | 12 | 1 | 12 | Nov 9, 2021 12:55 PM |
| P2 | Radius server is not responding. | ACCESS | Device | 2 | 1 | 1 | Nov 3, 2021 2:26 PM |

2. The **Layer 2 loop symptoms** slide-in pane displays all associated issues per device. Click the **Host flaps observed in 1 VLAN(s)** link under the Issues column for a device.

**Figure 14 Cisco DNA Center Issues–Layer 2 Loop Symptoms**



Layer 2 loop symptoms

Nov 3, 2021 12:00 PM - Nov 10, 2021 3:00 PM | Global

12 Open Issues

1 Area
1 Buildings, 3 Floors

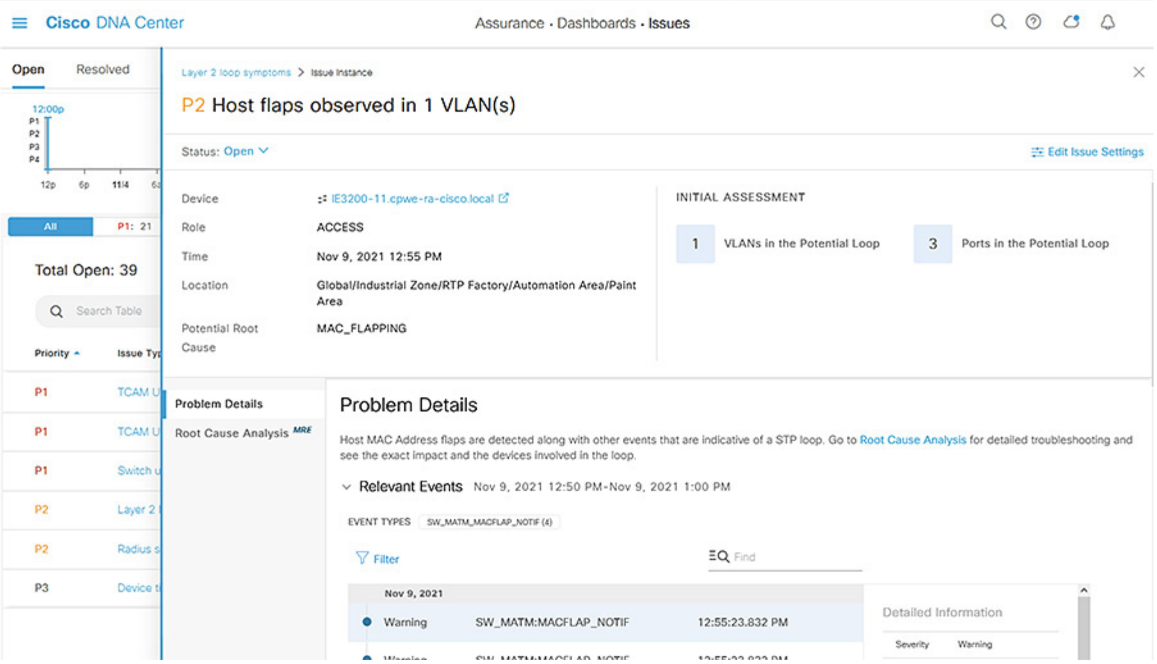
12 ACCESS

0 Selected

| ☐ Issue | Site | Device | Device Type |
|---|---|---|---|
| ☐ Host flaps observed in 1 VLAN(s) | Industrial Zone/RTP Factory/Automation Area/Paint Area | IE3200-11.cpwe-ra-cisco.local | Cisco Catalyst IE-3200-: |
| ☐ Host flaps observed in 1 VLAN(s) | Industrial Zone/RTP Factory/Automation Area/Paint Area | IE3200-3.cpwe-ra-cisco.local | Cisco Catalyst IE-3200-: |
| ☐ Host flaps observed in 1 VLAN(s) | Industrial Zone/RTP Factory/Automation Area/Paint Area | IE3200-10.cpwe-ra-cisco.local | Cisco Catalyst IE-3200-: |
| ☐ Host flaps observed in 1 VLAN(s) | Industrial Zone/RTP Factory/Automation Area/Distribution Switches | P5-9300-2.cpwe-ra-cisco.local | Cisco Catalyst 9300 Swi |
| ☐ Host flaps observed in 1 VLAN(s) | Industrial Zone/RTP Factory/Automation Area/Paint Area | IE3200-2.cpwe-ra-cisco.local | Cisco Catalyst IE-3200-: |

3. The **Issue Instance** slide-in pane will display details about the occurrence of the issue including time and associated events.

**Figure 15 Cisco DNA Center Issues–Host Flaps**



Total Open: 39

| Priority | Issue Typ |
|---|---|
| P1 | TCAM U |
| P1 | TCAM U |
| P1 | Switch u |
| P2 | Layer 2 |
| P2 | Radius s |
| P3 | Device t |

P2 Host flaps observed in 1 VLAN(s)

Status: Open

| | |
|---|---|
| Device | IE3200-11.cpwe-ra-cisco.local |
| Role | ACCESS |
| Time | Nov 9, 2021 12:55 PM |
| Location | Global/Industrial Zone/RTP Factory/Automation Area/Paint Area |
| Potential Root Cause | MAC_FLAPPING |

INITIAL ASSESSMENT

1 VLANs in the Potential Loop

3 Ports in the Potential Loop

Problem Details

Host MAC Address flaps are detected along with other events that are indicative of a STP loop. Go to Root Cause Analysis for detailed troubleshooting and see the exact impact and the devices involved in the loop.

Relevant Events Nov 9, 2021 12:50 PM-Nov 9, 2021 1:00 PM

EVENT TYPES SW_MATM_MACFLAP_NOTIF (4)

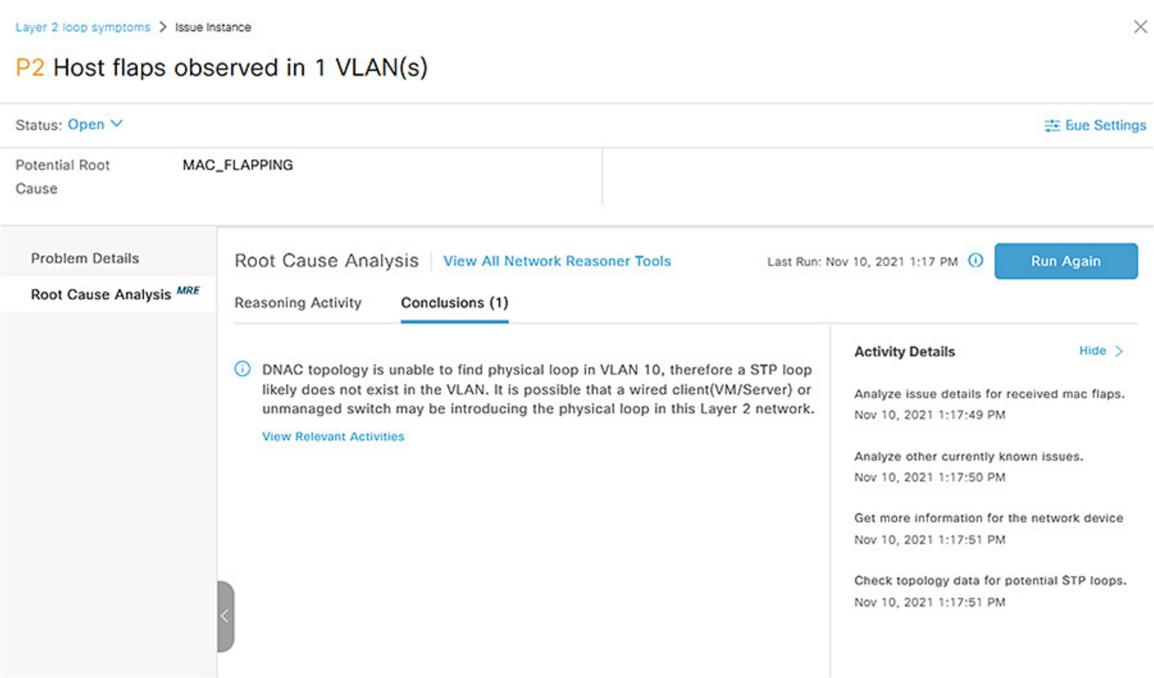
Nov 9, 2021

| | | |
|---|---|---|
| Warning | SW_MATM:MACFLAP_NOTIF | 12:55:23.832 PM |

Severity Warning

4. Click the **Root Cause Analysis** tab on the left side bar and click the **Run Machine Reasoning** button. Cisco DNA Center will run an automated analysis of telemetry data to help determine issue cause and suggest remediation. Click the **View Details** button when it finishes.

**Figure 16 Cisco DNA Center MRE**



P2 Host flaps observed in 1 VLAN(s)

Status: Open

Potential Root Cause MAC_FLAPPING

Root Cause Analysis

Last Run: Nov 10, 2021 1:17 PM

DNAC topology is unable to find physical loop in VLAN 10, therefore a STP loop likely does not exist in the VLAN. It is possible that a wired client(VM/Server) or unmanaged switch may be introducing the physical loop in this Layer 2 network.

View Relevant Activities

Analyze issue details for received mac flaps.
Nov 10, 2021 1:17:49 PM

Analyze other currently known issues.
Nov 10, 2021 1:17:50 PM

Get more information for the network device
Nov 10, 2021 1:17:51 PM

Check topology data for potential STP loops.
Nov 10, 2021 1:17:51 PM

# Security

## Cisco DNA Center

For configuring Cisco DNA Center in a secure manner, refer to the Cisco DNA Center Security Best Practices Guide: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/hardening_guide/b_dnac_security_best_practices_guide.html.

## Industrial Automation Network Infrastructure

Cisco DNA Center can help manage the security of your network infrastructure with device configuration as well as applying network controls through the integration with Cisco ISE. The process is as follows:

1. Connect Cisco DNA Center to ISE. Note that ISE can also be integrated with Cisco Cyber Vision to provide context for profiling industrial endpoints.
2. Define SGTs and TrustSec policy in Cisco DNA Center.
3. Define Profiles, and Authentication and Authorization policies in ISE.
4. Update Network Settings and Telemetry in Cisco DNA Center for all desired Sites to include AAA and IP Device Tracking and update necessary templates for additional TrustSec settings (interface configuration, SXP, enforcement, and so on).
5. Send NetFlow to Cisco DNA Center (configuration pushed through Templates).
6. Provision devices to apply the configurations and establish device communication with ISE, using AAA in Network Settings as well as additional template configurations.

For a full overview of the ISE and TrustSec implementation and recommendations in the Industrial Automation architecture, refer to the Industrial Automation Design Guide: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG.html.

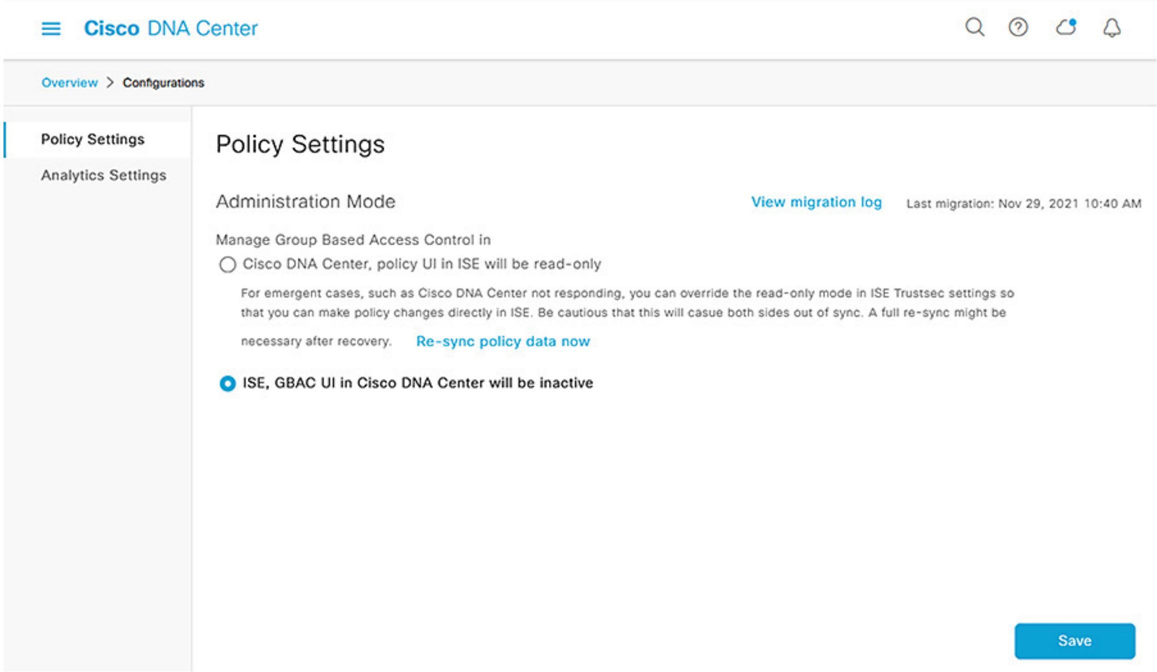
### Cisco DNA Center and ISE

Cisco DNA Center integrates with Cisco ISE to establish unified environment tracking and control. When provisioning a device through Cisco DNA Center, AAA and RADIUS can be added to the Site's network settings to automatically configure the necessary features for the device to communicate with Cisco ISE. IP device tracking can be enabled in Telemetry settings as well to track endpoint IP address to SGT bindings (see Network Settings). In addition, Cisco DNA Center will populate the network device database in ISE with the new device to establish the communication. Further configuration for AAA, such as policy maps and interface configurations, can be done through Day-N templates. See the Appendix for an example TrustSec template configuration for an IA architecture.

After integrating with ISE, it is recommended to use Cisco DNA Center as the TrustSec authority. The TrustSec policy matrix and SGT scheme are created and managed from Cisco DNA Center and the updates are automatically communicated to ISE, however ISE will maintain the profiling, authentication, and authorization policies. For existing ISE deployments, Cisco DNA Center will read the TrustSec configurations from ISE and management can be done from Cisco DNA Center. Note that Cisco DNA Center does not support multiple TrustSec matrices and if necessary TrustSec can be managed by ISE instead of Cisco DNA Center.

The authority can be changed by navigating to **Policy > Group-Based Access Control** and clicking the **Configuration** link.

**Figure 17 Cisco DNA Center Policy Settings**



Policy Settings

Administration Mode

Last migration: Nov 29, 2021 10:40 AM

Manage Group Based Access Control in

○ Cisco DNA Center, policy UI in ISE will be read-only

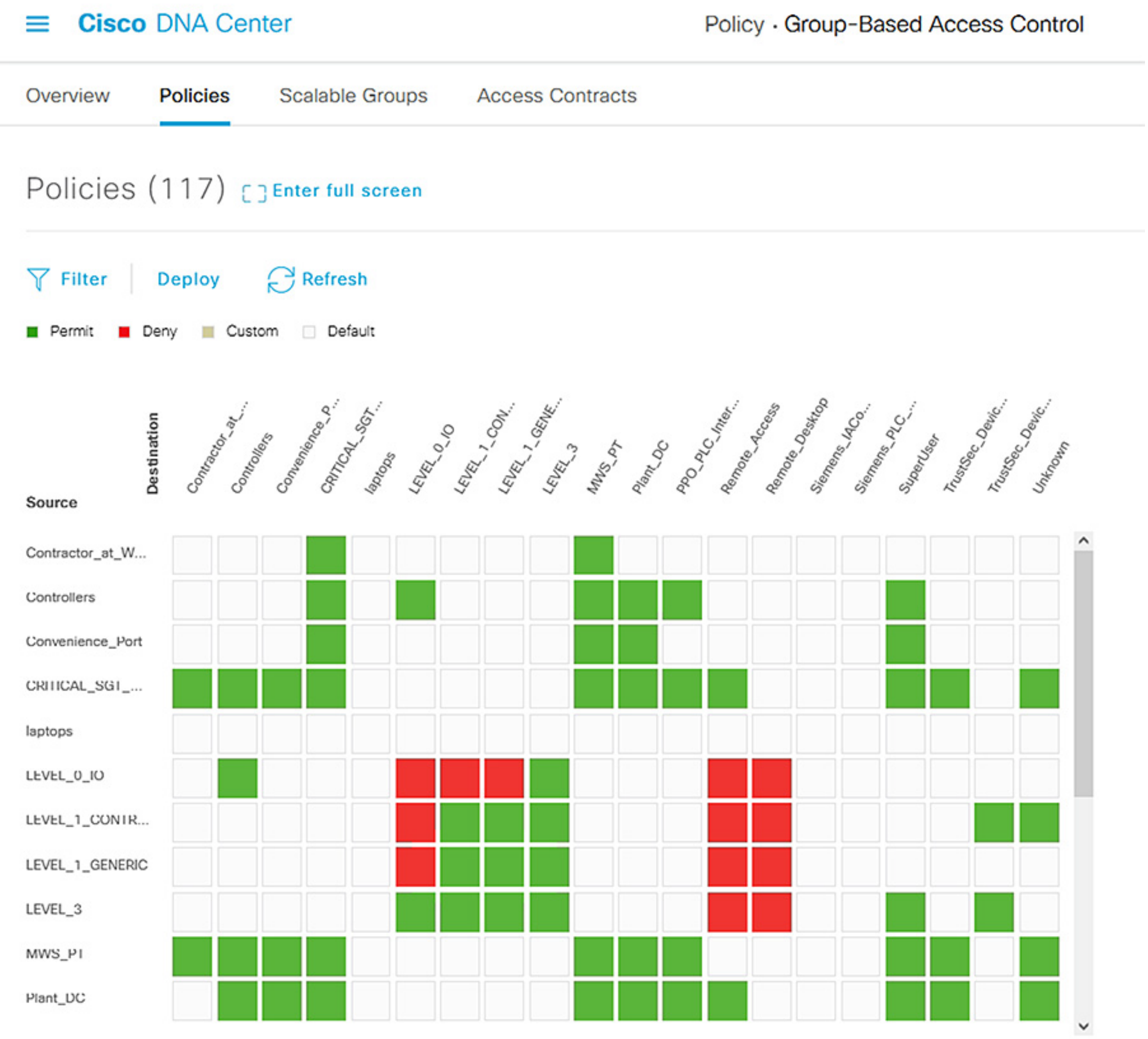
For emergent cases, such as Cisco DNA Center not responding, you can override the read-only mode in ISE Trustsec settings so that you can make policy changes directly in ISE. Be cautious that this will casue both sides out of sync. A full re-sync might be necessary after recovery. Re-sync policy data now

● ISE, GBAC UI in Cisco DNA Center will be inactive

After creating the SGTs in Cisco DNA Center, the policy matrix can be updated to suit the enforcement intent. To make changes to the TrustSec policy matrix in DNA Center, do the following:

1. From the Cisco DNA Center web interface, navigate to **Policy > Group-Based Access Control**.
2. Click the **Policies** tab.
3. Click the square of the source and destination pair for which there needs to be a permit or deny contract.
4. On the **Create Policy** slide-in pane, click the **Change Contract** link and choose the appropriate option (**Permit IP, Deny IP**, and so on). Click the **Change** button.
5. Click the **Deploy** link at the top of the matrix.

**Figure 18 Cisco DNA Center TrustSec Policy Matrix**



Policies (117)

🟩 Permit 🟥 Deny ▨ Custom □ Default

| Destination<br>Source | Contractor_at_... | Controllers | Convenience_P... | CRITICAL_SGT... | laptops | LEVEL_0_IO | LEVEL_1_CON... | LEVEL_1_GENE... | LEVEL_3 | MWS_PT | Plant_DC | PPO_PLC_Inter... | Remote_Access | Remote_Desktop | Siemens_IACo... | Siemens_PLC_... | SuperUser | TrustSec_Devic... | TrustSec_Devic... | Unknown |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Contractor_at_W... | □ | □ | □ | 🟩 | □ | □ | □ | □ | □ | 🟩 | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ |
| Controllers | □ | □ | □ | 🟩 | □ | 🟩 | □ | □ | □ | 🟩 | 🟩 | 🟩 | □ | □ | □ | □ | 🟩 | □ | □ | □ |
| Convenience_Port | □ | □ | □ | 🟩 | □ | □ | □ | □ | □ | 🟩 | 🟩 | □ | □ | □ | □ | □ | 🟩 | □ | □ | □ |
| CRITICAL_SGT_... | 🟩 | 🟩 | 🟩 | 🟩 | □ | □ | □ | □ | □ | 🟩 | 🟩 | 🟩 | 🟩 | □ | □ | □ | 🟩 | 🟩 | □ | 🟩 |
| laptops | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ |
| LEVEL_0_IO | □ | 🟩 | □ | □ | □ | 🟥 | 🟥 | 🟥 | 🟩 | □ | □ | □ | 🟥 | 🟥 | □ | □ | □ | □ | □ | □ |
| LEVEL_1_CONTR... | □ | □ | □ | □ | □ | 🟥 | 🟩 | 🟩 | 🟩 | □ | □ | □ | 🟥 | 🟥 | □ | □ | □ | □ | 🟩 | 🟩 |
| LEVEL_1_GENERIC | □ | □ | □ | □ | □ | 🟥 | 🟩 | 🟩 | 🟩 | □ | □ | □ | 🟥 | 🟥 | □ | □ | □ | □ | □ | □ |
| LEVEL_3 | □ | □ | □ | □ | □ | 🟩 | 🟩 | 🟩 | 🟩 | □ | □ | □ | 🟥 | 🟥 | □ | □ | 🟩 | □ | 🟩 | □ |
| MWS_PT | 🟩 | 🟩 | 🟩 | 🟩 | □ | □ | □ | □ | □ | 🟩 | 🟩 | 🟩 | □ | □ | □ | □ | 🟩 | 🟩 | □ | 🟩 |
| Plant_DC | □ | 🟩 | 🟩 | 🟩 | □ | □ | □ | □ | □ | 🟩 | 🟩 | 🟩 | 🟩 | □ | □ | □ | 🟩 | 🟩 | □ | 🟩 |

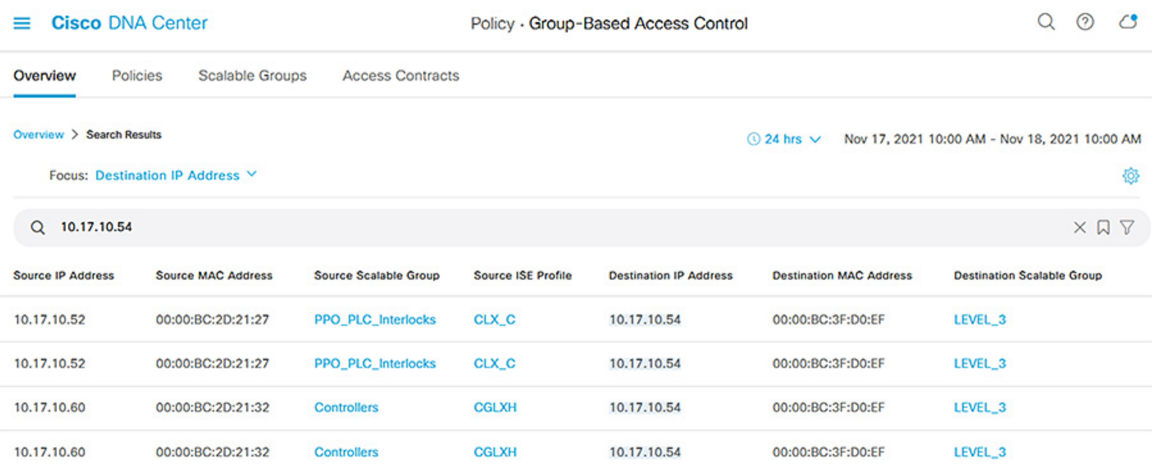
## Policy Analytics

Cisco DNA Center can help track communication flows from devices with NetFlow and TrustSec, giving administrators details about status and health to maintain accurate configuration and security posture.

After configuring Cisco DNA Center as a NetFlow collector through templates, communication flows can be reviewed by doing the following:

1. From the Cisco DNA Center web interface, navigate to **Policy > Group-Based Access Control**.
2. Under **View traffic for...**, click the **Scalable Groups** button.
3. The **Explore Scalable Groups** graphic shows SGT to SGT communications. Click a connection line to display further details.
4. Alternatively, from the **Policy > Group-Based Access Control** page enter the IP or MAC address of a device in the search bar and choose either the **Source IP Address** or **Destination IP Address** option from the drop-down list, then press **Return**. The **Search Results** table will show communication details for the device in question. Click the **24 hrs** button to change the date or time to view additional results.

**Figure 19 Cisco DNA Center Group-Based Access Control**


Cisco DNA Center
Policy · Group-Based Access Control
Overview
Policies
Scalable Groups
Access Contracts
Overview > Search Results
24 hrs
Nov 17, 2021 10:00 AM - Nov 18, 2021 10:00 AM
Focus: Destination IP Address

10.17.10.54

| Source IP Address | Source MAC Address | Source Scalable Group | Source ISE Profile | Destination IP Address | Destination MAC Address | Destination Scalable Group |
|---|---|---|---|---|---|---|
| 10.17.10.52 | 00:00:BC:2D:21:27 | PPO_PLC_Interlocks | CLX_C | 10.17.10.54 | 00:00:BC:3F:D0:EF | LEVEL_3 |
| 10.17.10.52 | 00:00:BC:2D:21:27 | PPO_PLC_Interlocks | CLX_C | 10.17.10.54 | 00:00:BC:3F:D0:EF | LEVEL_3 |
| 10.17.10.60 | 00:00:BC:2D:21:32 | Controllers | CGLXH | 10.17.10.54 | 00:00:BC:3F:D0:EF | LEVEL_3 |
| 10.17.10.60 | 00:00:BC:2D:21:32 | Controllers | CGLXH | 10.17.10.54 | 00:00:BC:3F:D0:EF | LEVEL_3 |

## Endpoint Analytics

In addition, endpoint details are monitored through Cisco DNA Center if the endpoint is connected to a switch managed by Cisco DNA Center, authenticated, and has a live session with ISE. To view endpoint analytics, do the following:

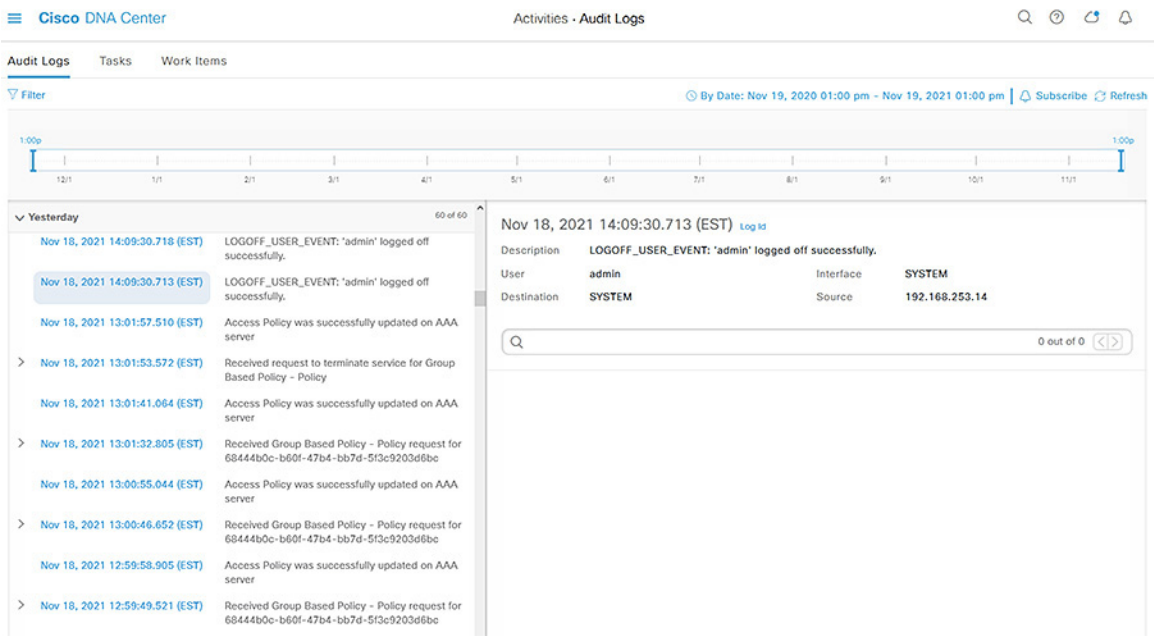
1. From the Cisco DNA Center web interface, navigate to **Policy > AI Endpoint Analytics**.
2. Click the **Endpoint Inventory** tab.
3. Click the link in the **MAC Address** column to view further details about the endpoint.

# Additional Tools and Troubleshooting

## Audit Logs and Tasks

Cisco DNA Center tracks many activities done in the tool. Audit Logs provide details such as user logins, data purges, device name changes, and so on. The Tasks tool shows real-time status details for activities launched by users, such as provisioning, software update, replacement workflow, and so on. From the Cisco DNA Center web interface, navigate to **Activities** from the main menu to view Audit Logs and Tasks.

**Figure 20 Cisco DNA Center Audit Logs**



Nov 18, 2021 14:09:30.718 (EST) LOGOFF_USER_EVENT: 'admin' logged off successfully.

Nov 18, 2021 14:09:30.713 (EST) LOGOFF_USER_EVENT: 'admin' logged off successfully.

Nov 18, 2021 13:01:57.510 (EST) Access Policy was successfully updated on AAA server

Nov 18, 2021 13:01:53.572 (EST) Received request to terminate service for Group Based Policy - Policy

Nov 18, 2021 13:01:41.064 (EST) Access Policy was successfully updated on AAA server

Nov 18, 2021 13:01:32.805 (EST) Received Group Based Policy - Policy request for 68444b0c-b60f-47b4-bb7d-5f3c9203d6bc

Nov 18, 2021 13:00:55.044 (EST) Access Policy was successfully updated on AAA server

Nov 18, 2021 13:00:46.652 (EST) Received Group Based Policy - Policy request for 68444b0c-b60f-47b4-bb7d-5f3c9203d6bc

Nov 18, 2021 12:59:58.905 (EST) Access Policy was successfully updated on AAA server

Nov 18, 2021 12:59:49.521 (EST) Received Group Based Policy - Policy request for 68444b0c-b60f-47b4-bb7d-5f3c9203d6bc

Nov 18, 2021 14:09:30.713 (EST)

Description LOGOFF_USER_EVENT: 'admin' logged off successfully.

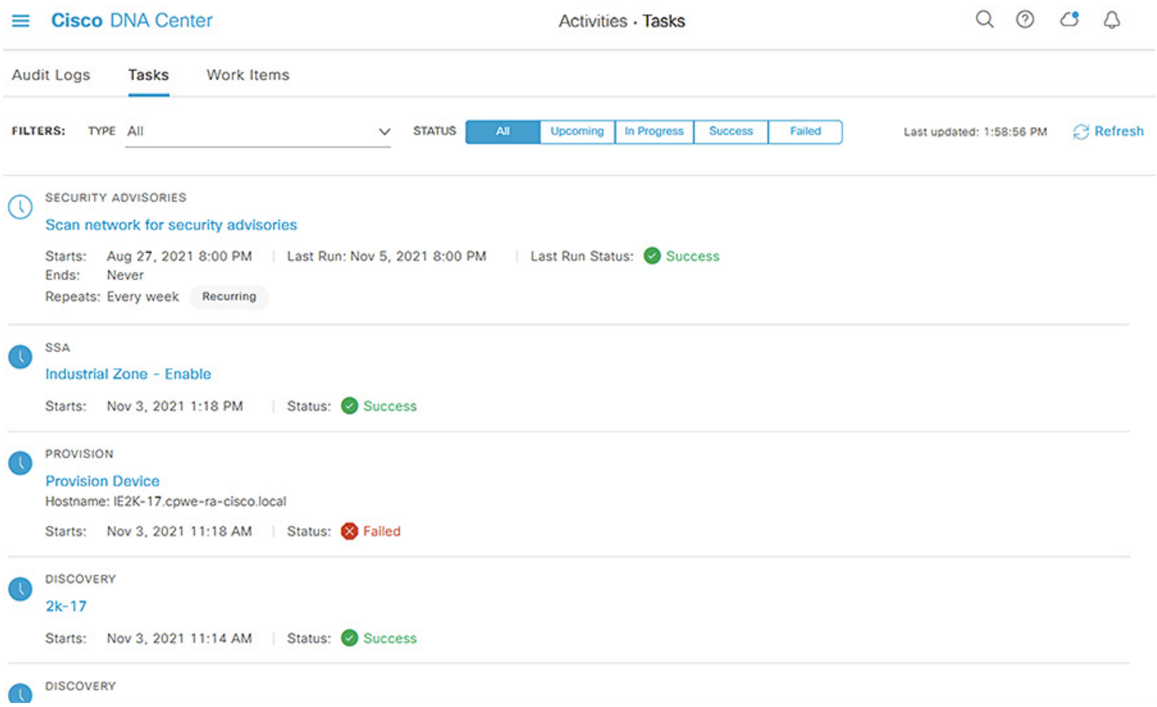
User admin

Interface SYSTEM

Destination SYSTEM

Source 192.168.253.14

**Figure 21 Cisco DNA Center Tasks**



FILTERS: TYPE All

STATUS All | Upcoming | In Progress | Success | Failed

Last updated: 1:58:56 PM

SECURITY ADVISORIES

Scan network for security advisories

Starts: Aug 27, 2021 8:00 PM | Last Run: Nov 5, 2021 8:00 PM | Last Run Status: Success

Ends: Never

Repeats: Every week

SSA

Industrial Zone - Enable

Starts: Nov 3, 2021 1:18 PM | Status: Success

PROVISION

Provision Device

Hostname: IE2K-17.cpwe-ra-cisco.local

Starts: Nov 3, 2021 11:18 AM | Status: Failed

DISCOVERY

2k-17

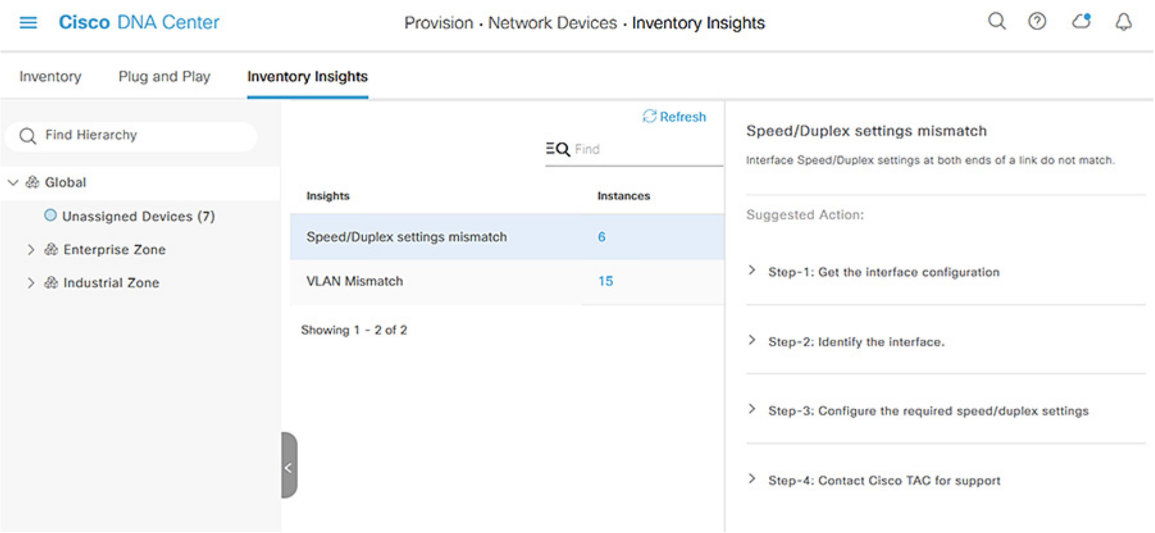
Starts: Nov 3, 2021 11:14 AM | Status: Success

DISCOVERY

# Inventory Insights

Because Cisco DNA Center is collecting real time data about devices and their activity, it can help highlight potential issues. By navigating to **Provision > Network Devices > Inventory Insights**, you can see a consolidated view potential issues and remediation suggestions on a per-Site basis.

**Figure 22 Cisco DNA Center Inventory Insights**



| Insights | Instances |
|---|---|
| Speed/Duplex settings mismatch | 6 |
| VLAN Mismatch | 15 |

Showing 1 - 2 of 2

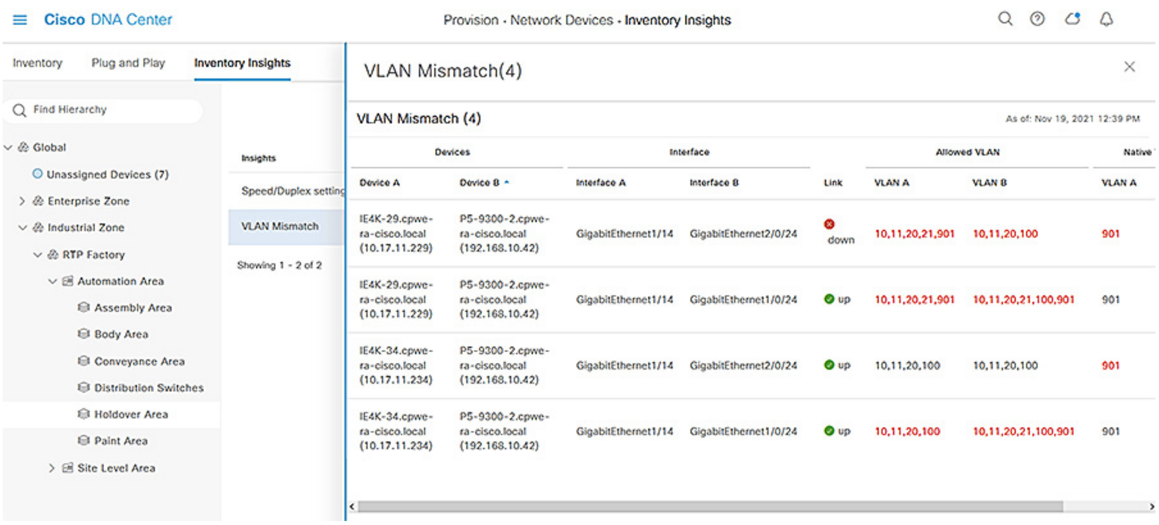
Speed/Duplex settings mismatch

Interface Speed/Duplex settings at both ends of a link do not match.

Suggested Action:

- Step-1: Get the interface configuration
- Step-2: Identify the interface.
- Step-3: Configure the required speed/duplex settings
- Step-4: Contact Cisco TAC for support

**Figure 23 Cisco DNA Center Inventory Insights Details**



VLAN Mismatch(4)

VLAN Mismatch (4)

As of: Nov 19, 2021 12:39 PM

| Devices | | Interface | | | Allowed VLAN | | Native |
|---|---|---|---|---|---|---|---|
| Device A | Device B | Interface A | Interface B | Link | VLAN A | VLAN B | VLAN A |
| IE4K-29.cpwe-ra-cisco.local (10.17.11.229) | P5-9300-2.cpwe-ra-cisco.local (192.168.10.42) | GigabitEthernet1/14 | GigabitEthernet2/0/24 | down | 10,11,20,21,901 | 10,11,20,100 | 901 |
| IE4K-29.cpwe-ra-cisco.local (10.17.11.229) | P5-9300-2.cpwe-ra-cisco.local (192.168.10.42) | GigabitEthernet1/14 | GigabitEthernet1/0/24 | up | 10,11,20,21,901 | 10,11,20,21,100,901 | 901 |
| IE4K-34.cpwe-ra-cisco.local (10.17.11.234) | P5-9300-2.cpwe-ra-cisco.local (192.168.10.42) | GigabitEthernet1/14 | GigabitEthernet2/0/24 | up | 10,11,20,100 | 10,11,20,100 | 901 |
| IE4K-34.cpwe-ra-cisco.local (10.17.11.234) | P5-9300-2.cpwe-ra-cisco.local (192.168.10.42) | GigabitEthernet1/14 | GigabitEthernet1/0/24 | up | 10,11,20,100 | 10,11,20,21,100,901 | 901 |

# Command Runner

Cisco DNA Center provides a quick way to run commands on a device directly From the Cisco DNA Center web interface, which can be helpful for verifying configuration without having to access the device directly. To launch Command Runner, do the following:

1. From the Cisco DNA Center web interface, navigate to **Provision > Network Devices > Inventory**.
2. From the left Hierarchy, choose the Site for the device in question.
3. Click the link for the device under the **Device Name** column.
4. On the **Device** page, click the **Run Commands** link.

**Note:** Only User EXEC level commands are accepted in Command Runner.

## License Manager

Cisco DNA Center keeps track of the licensing for the managed devices, which can help administrators verify compliance and troubleshoot issues pertaining to inadequate licensing. Navigate to **Tools > License Manager** to view the licensing details.

## Security Advisories

Because Cisco DNA Center communicates with Cisco.com directly for software image management, it has an up-to-date database of publicized security advisories associated to specific software images. **Tools > Security Advisories** displays a table of advisory IDs and lists any managed devices that are affected.

## Reports

Cisco DNA Center has specialized reports to organize its data into useful insights. Navigate to **Reports > Report Templates** to browse the available reports that can be generated into various formats such as PDF, CSV, JSON, and so on.

## System 360

Cisco DNA Center provides its own health status and details in a unique dashboard, which can help provide insight into software upkeep, integration health, and so on. Navigate to **System > System 360** to view the **System Management** dashboard.

# Appendix

## Plug and Play Network Preparation

When adding a new switch to the network, there are some configuration prerequisites for Plug and Play to be able to run successfully, including:

- PNP VLAN—The upstream switch needs to have the Plug and Play VLAN specified.

```
Switch(config)#pnp startup-vlan pnp_vlan_number
```

- Interface configuration—The interface to which the new switch is connected needs to be configured with the PNP startup VLAN. For example:

```
Switch(config-if)#switchport trunk allowed vlan pnp_vlan_number
```

- DHCP for the PNP switch—The switch being added to the network needs to receive a DHCP IP address for communication with Cisco DNA Center. On the DHCP server, configure a DHCP pool, such as:

```
Switch(config)#ip dhcp pool ZTD-switches
Switch(dhcp-config)#network 100.0.0.0 255.255.252.0
Switch(dhcp-config)#bootfile remember
Switch(dhcp-config)#default-router 100.0.0.2
Switch(dhcp-config)#option 43 ascii "5A1D;B2;K4;I10.13.48.131;J80"
Switch(dhcp-config)#remember
```

The DHCP option 43 string has the following components, delimited by semi-colons:

- 5A1N;—Specifies the DHCP sub-option for PnP, active operation, version 1, no debug information. It is not necessary to change this part of the string.
- B2;—IP address type. B2 stands for IPv4. B1 should be used for hostname.
- Ixxx.xxx.xxx.xxx;—IP address or hostname of the Cisco DNA Center controller (following a capital letter i). In this example, the IP address is 172.19.45.222.
- Jxxxx—Port number to use to connect to the Cisco DNA Center controller. In this example, the port number is 80. The default is port 80 for HTTP and port 443 for HTTPS.
- K4;—Transport protocol to be used between the device and the controller. Use K4 for HTTP (default) or K5 for HTTPS.

There is a DNS discovery option similar to DHCP which requires the following:

- Domain name option configured on DHCP server.
- DNS server option configured on DHCP server.
- PnP server (Cisco DNA Center) resolves to PnP deployment server IP address in DNS.
- IP helper address should be configured on the distribution switch.

# Offline Discovery Example Switch Configuration

```
Switch(config)#username user privilege 15 password 0 password

Switch(config)#enable secret 5 $1$yXVL$XckjPL0xYiab7A/wxAe8N.
Switch(config)#enable password 7 04785A150C2E1D1C5A

Switch(config)#vlan 100
Switch(config)#interface vlan 100
Switch(config-if)#ip address 100.0.0.3 255.255.252.0

Switch(config)#interface GigabitEthernet1/1
Switch(config-if)#switchport trunk allowed vlan 21,100
Switch(config-if)#switchport mode trunk

Switch(config)#ip default-gateway 100.0.0.2


Switch(config)#ip ssh version 2
Switch(config)#line vty 0 15
Switch(config-line)#login local
Switch(config-line)#transport input all
Switch(config-line)#transport preferred none
```

# Cisco DNA Center Template Examples for the Industrial Automation Network

Any example provided is for reference only and should be adapted to the customer environment. Examples are based on the Cisco IE3400 switch.

## Onboarding Template

For onboarding, the main goal is to get the device online with a base configuration; this is the initial configuration pushed out as part of the PnP process.

The following is an example for a device connected via EtherChannel, requires a native VLAN different than 1, requires CTS inline tagging, and requires a static IP address.

```
hostname $hostname

vlan $vlanList
!
interface vlan $mgmtVlan
ip address $mgmtIp $mgmtMask


interface Port-channel1
switchport trunk allowed vlan $vlanList
switchport trunk native vlan 900
switchport mode trunk

!
interface range $uplinkRange
switchport mode trunk
switchport trunk allowed vlan $vlanList
switchport trunk native vlan 900
cts manual
  policy static sgt 3040 trusted
channel-group 1 mode desirable


ip default-gateway $gateway

!
line con 0
logging synchronous
line vty 0 4
exec-timeout 0 0
privilege level 15
transport preferred none
transport input ssh
line vty 5 15
!

end
```

## Day-N Templates

For Day-N configuration, the main goal is to complete the device configuration so it is ready for production. The format can be a standard template or a composite template.

### Example for General Configuration on the Cisco IE3400 Switch

```
#####VLANS
vlan $vlanList

interface vlan$sviVlan
ip address $ipAddress $mask

###IGMP
ip igmp snooping querier

####Netflow. Collector should point to DNAC for policy analytics

flow record dnacrecord
 match ipv4 protocol
 match datalink mac source address input
 match datalink mac destination address input
 match ipv4 tos
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect flow cts source group-tag
 collect flow cts destination group-tag

flow exporter dnacexporter
 destination $netflowCollector
 source $sourceVlan
 transport udp $netflowPort
 option interface-table timeout 10
 option vrf-table timeout 10
 option sampler-table
 option application-table timeout 10
!
flow monitor dnacmonitor
 exporter dnacexporter
 record dnacrecord
 cache timeout inactive 600
 cache timeout active 1800

 ####Alarms

alarm-profile defaultPort
 alarm link-fault not-operating fcs-error
 syslog link-fault not-operating fcs-error
 notifies link-fault not-operating fcs-error
!
alarm facility sd-card enable
alarm facility sd-card syslog
alarm facility sd-card notifies
alarm facility temperature primary relay major
alarm facility temperature primary syslog
alarm facility temperature primary notifies
alarm facility temperature primary low 0
alarm facility temperature primary high 80

######Error Disable
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause psecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause arp-inspection
errdisable recovery cause loopback
errdisable recovery interval 30
```

```
### Enable aggressive mode UDLD on all fiber uplinks
udld aggressive


#####AAA Policy

class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match result-type aaa-timeout
 match authorization-status authorized
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match result-type aaa-timeout
 match authorization-status unauthorized
!
class-map type control subscriber match-all AI_IN_CRITICALSGT_AUTH
 match activated-service-template IA_CRITICAL_SGT
!
class-map type control subscriber match-none AI_NOT_IN_CRITICALSGT_AUTH
 match activated-service-template IA_CRITICAL_SGT
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
 match authorizing-method-priority gt 20
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
 match result-type method dot1x method-timeout
!
class-map type control subscriber match-any IA_CRITICAL_SGT
 match activated-service-template IA_CRITICAL_SGT
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
policy-map type control subscriber IA_DOT1X_MAB_POLICIES
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab retries 3 retry-time 0 priority 10
   20 authenticate using dot1x retries 3 retry-time 0
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template IA_CRITICAL_SGT
   20 authorize
   30 authentication-restart 60
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 authentication-restart 5
   20 authorize
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
  60 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 10
 event aaa-available match-first
  10 class AI_IN_CRITICALSGT_AUTH do-until-failure
   10 clear-session
  20 class AI_NOT_IN_CRITICALSGT_AUTH do-until-failure
   10 resume reauthentication
 event violation match-all
  10 class always do-until-failure
   10 restrict

#####QoS

access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
!
policy-map CIP-PTP-Traffic
class CIP-Implicit_dscp_55
set ip dscp 55
class CIP-Implicit_dscp_47
set ip dscp 47
class CIP-Implicit_dscp_43
set ip dscp 43
class CIP-Implicit_dscp_any
set ip dscp 31
class CIP-Other
set ip dscp 27
class 1588-PTP-Event
set ip dscp 59
class 1588-PTP-General
set ip dscp 47
!
policy-map PTP-Event-Priority
class class-0
priority
class class-1
bandwidth remaining percent 40
class class-2
bandwidth remaining percent 20
class class-default
bandwidth remaining percent 40
!
class-map match-all 1588-PTP-General
match access-group 107
class-map match-all 1588-PTP-Event
```

```
match access-group 106
class-map match-all CIP-Other
match access-group 105
class-map match-all CIP-Implicit_dscp_any
match access-group 104
class-map match-all CIP-Implicit_dscp_43
match access-group 103
class-map match-all CIP-Implicit_dscp_47
match access-group 102
class-map match-all CIP-Implicit_dscp_55
match access-group 101
!
class-map match-all class-2
match ip dscp ef
class-map match-all class-1
match ip dscp 47
class-map match-all class-0
match ip dscp 59
!
```

### Example for Interface Configuration

See tip in binding to define variables. This example shows how to configure interfaces using foreach loops:

```
#foreach($interface in $accessInterfaces)
interface $interface.portName
 description endpoint
 switchport access vlan $dataVlan
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 #if($netflowPolicy)
 ip flow monitor dnacmonitor input
 #end
 access-session port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
 service-policy type control subscriber IA_DOT1X_MAB_POLICIES
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
 #if($stormControl)
 storm-control broadcast level 3 1
 #end
 exit
 vlan $dataVlan
#end


#foreach($uplinkInterface in $trunkInterfaces)
interface $uplinkInterface.portName
 description trunk
 switchport trunk allowed vlan $vlans
 switchport mode trunk
 #if($cts)
  cts manual
  policy static sgt $uplinkSGT trusted
  exit
  exit
 #end
 vlan $vlans
#end
```

### Example for Cyber Vision Sensor Configuration

This example only configures iox if required by the user, after it waits for iox to start.

```
#if ($enable_iox == 1)
iox
#MODE_ENABLE
terminal shell
sleep 30
sleep 30
terminal no shell
#MODE_END_ENABLE
#end
vlan 2
remote-span
interface AppGigabitEthernet 1/1
switchport mode trunk
exit
monitor session 1 source interface $intRange
monitor session 1 destination remote vlan 2
monitor session 1 destination format-erspan 169.254.1.2
```

### Example for TrustSec Configuration

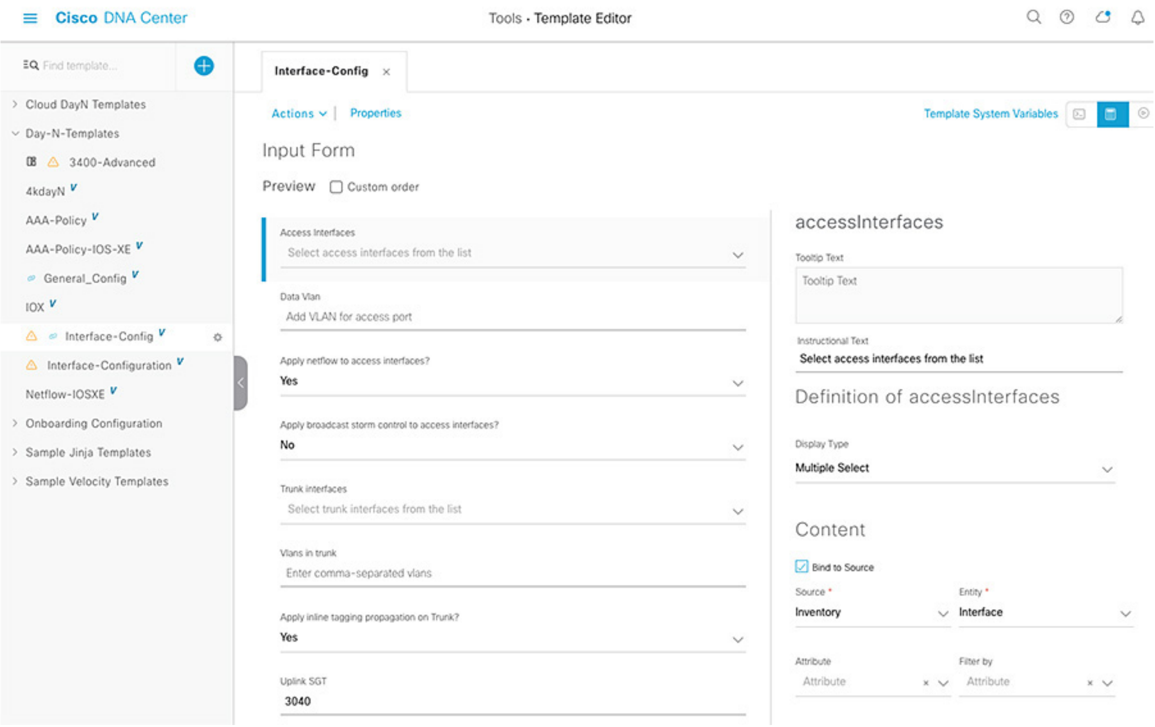
SXP and Enforcement:

```
####Trustsec SXP
cts sxp enable
cts sxp default password 0 $sharedKey
cts sxp connection peer $peerIP source $sourceIP.ipv4Address password default mode local speaker
hold-time 0

####Trustsec Enforcement

cts role-based enforcement
cts role-based enforcement vlan-list $vlanList
```

## Template Tips

1. Source-binding–Bind the details Cisco DNA Center has learned about the device (such as interface names) to a variable in the template.

Figure 24 Cisco DNA Center Template Editor–1



Input Form

Preview □ Custom order

Access Interfaces: Select access interfaces from the list

Data Vlan: Add VLAN for access port

Apply netflow to access interfaces?: Yes

Apply broadcast storm control to access interfaces?: No

Trunk interfaces: Select trunk interfaces from the list

Vlans in trunk: Enter comma-separated vlans

Apply inline tagging propagation on Trunk?: Yes

Uplink SGT: 3040

accessInterfaces

Tooltip Text: Tooltip Text

Instructional Text: Select access interfaces from the list

Definition of accessInterfaces

Display Type: Multiple Select

Content

☑ Bind to Source

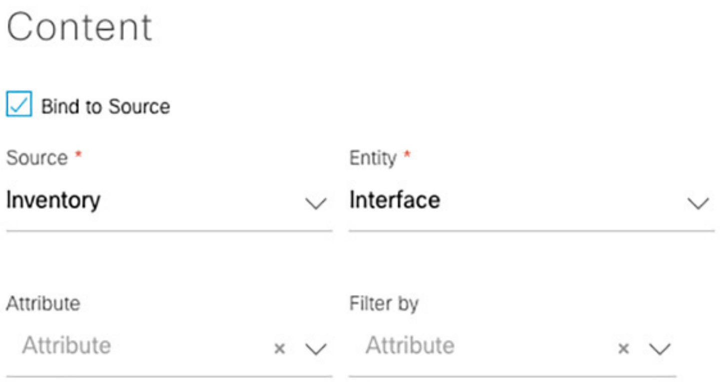
Source *: Inventory

Entity *: Interface

Attribute: Attribute

Filter by: Attribute

Figure 25 Cisco DNA Center Template Editor–2



Content

☑ Bind to Source

Source *: Inventory

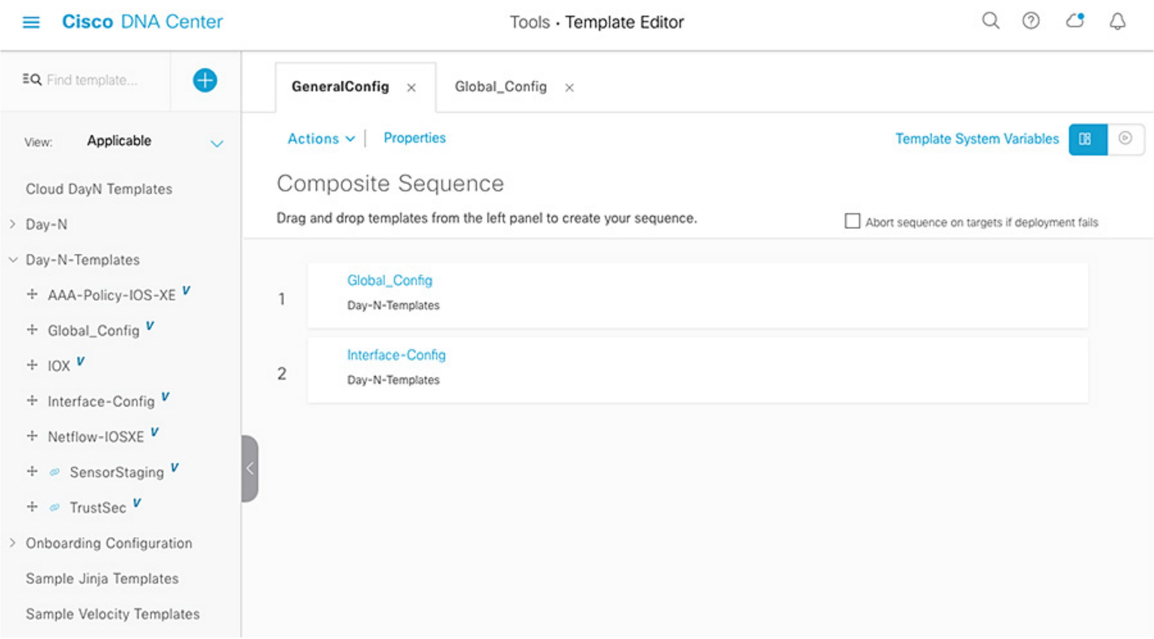
Entity *: Interface

Attribute: Attribute

Filter by: Attribute

2. Composite templates can be used to guarantee execution order.

Figure 26 Cisco DNA Center Composite Templates



Cisco DNA Center — Tools · Template Editor

Find template... — View: Applicable

- Cloud DayN Templates
- Day-N
- Day-N-Templates
  - AAA-Policy-IOS-XE V
  - Global_Config V
  - IOX V
  - Interface-Config V
  - Netflow-IOSXE V
  - SensorStaging V
  - TrustSec V
- Onboarding Configuration
- Sample Jinja Templates
- Sample Velocity Templates

Tabs: GeneralConfig | Global_Config — Actions | Properties — Template System Variables

Composite Sequence

Drag and drop templates from the left panel to create your sequence.

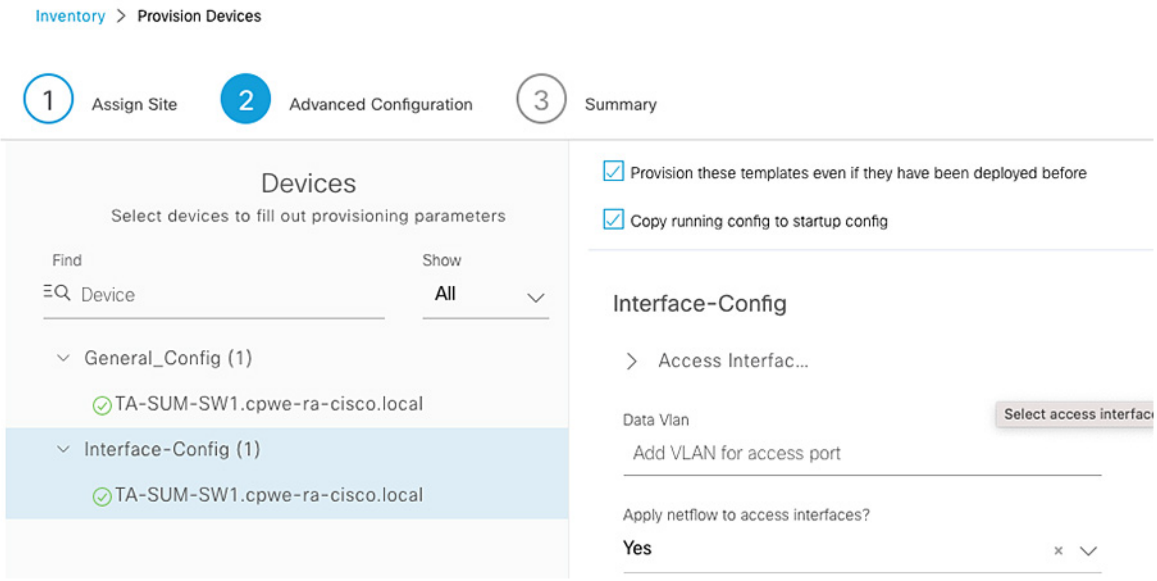
□ Abort sequence on targets if deployment fails

1 Global_Config — Day-N-Templates

2 Interface-Config — Day-N-Templates

3. Options–Check the **Provisioning of these templates even if they have been deployed before** and **Copy running config to startup config** checkboxes.

Figure 27 Cisco DNA Center Provisioning with Templates–1



Inventory > Provision Devices

1 Assign Site — 2 Advanced Configuration — 3 Summary

Devices

Select devices to fill out provisioning parameters

Find: Device — Show: All

- General_Config (1)
  - TA-SUM-SW1.cpwe-ra-cisco.local
- Interface-Config (1)
  - TA-SUM-SW1.cpwe-ra-cisco.local

☑ Provision these templates even if they have been deployed before

☑ Copy running config to startup config

Interface-Config

Access Interfac...

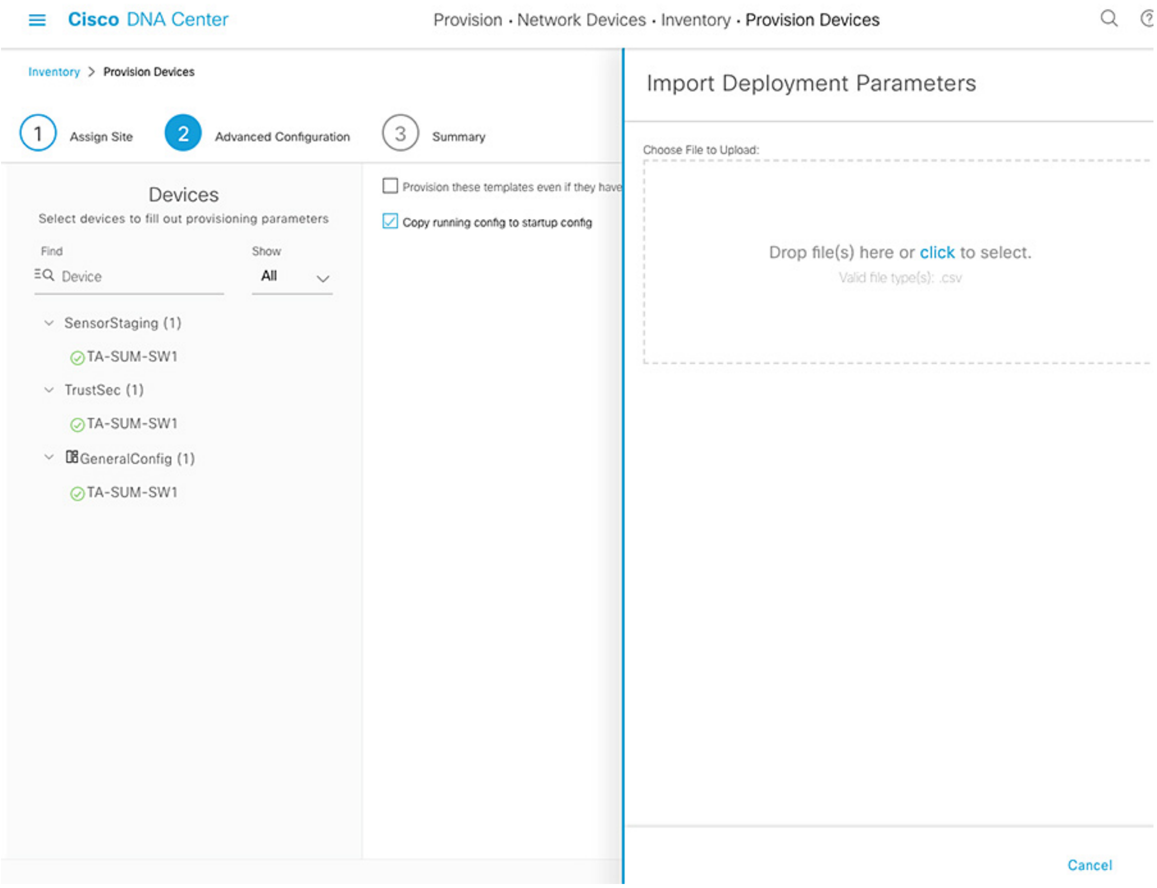
Data Vlan: Add VLAN for access port — Select access interfac

Apply netflow to access interfaces? Yes

4. Use files for variables.

Export file first to download sample, then fill and import. Re-use as needed.

**Figure 28 Cisco DNA Center Provisioning with Templates–2**

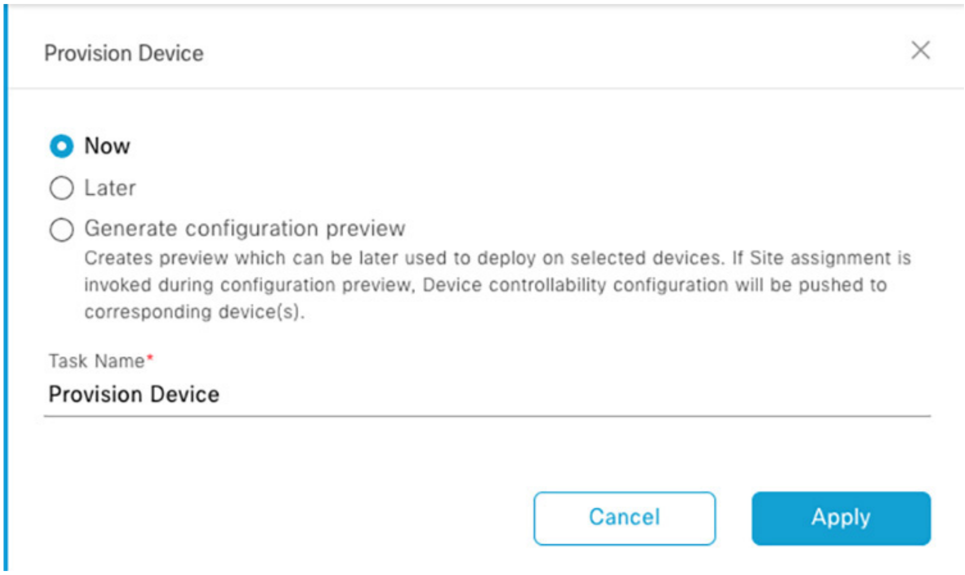


□ Provision these templates even if they have

☑ Copy running config to startup config

5. Generate a template preview.

**Figure 29 Cisco DNA Center Provisioning Preview–1**



Provision Device

● Now

○ Later

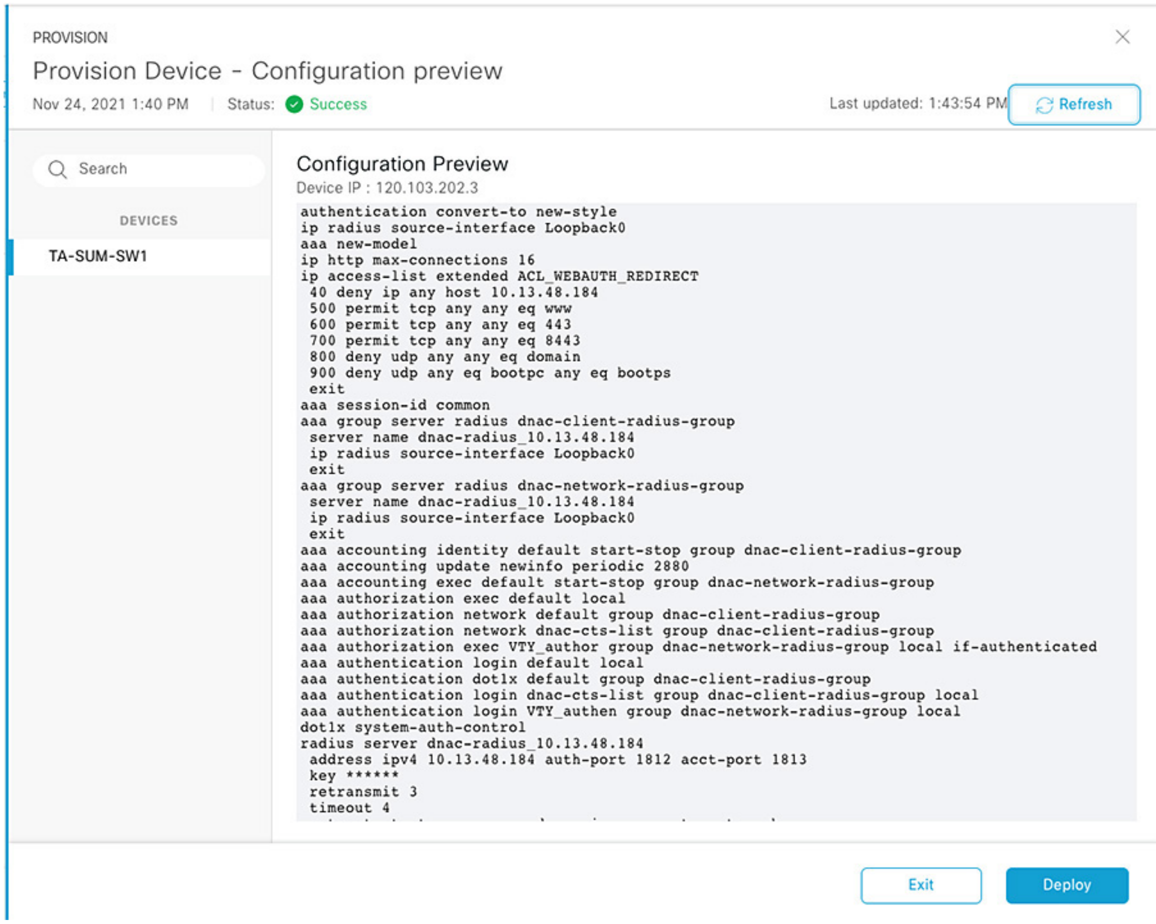
○ Generate configuration preview

Creates preview which can be later used to deploy on selected devices. If Site assignment is invoked during configuration preview, Device controllability configuration will be pushed to corresponding device(s).

Task Name*

Provision Device

**Figure 30 Cisco DNA Center Provisioning Preview–2**



PROVISION
Provision Device - Configuration preview
Nov 24, 2021 1:40 PM | Status: Success
Last updated: 1:43:54 PM
Refresh
Search
DEVICES
TA-SUM-SW1
Exit
Deploy

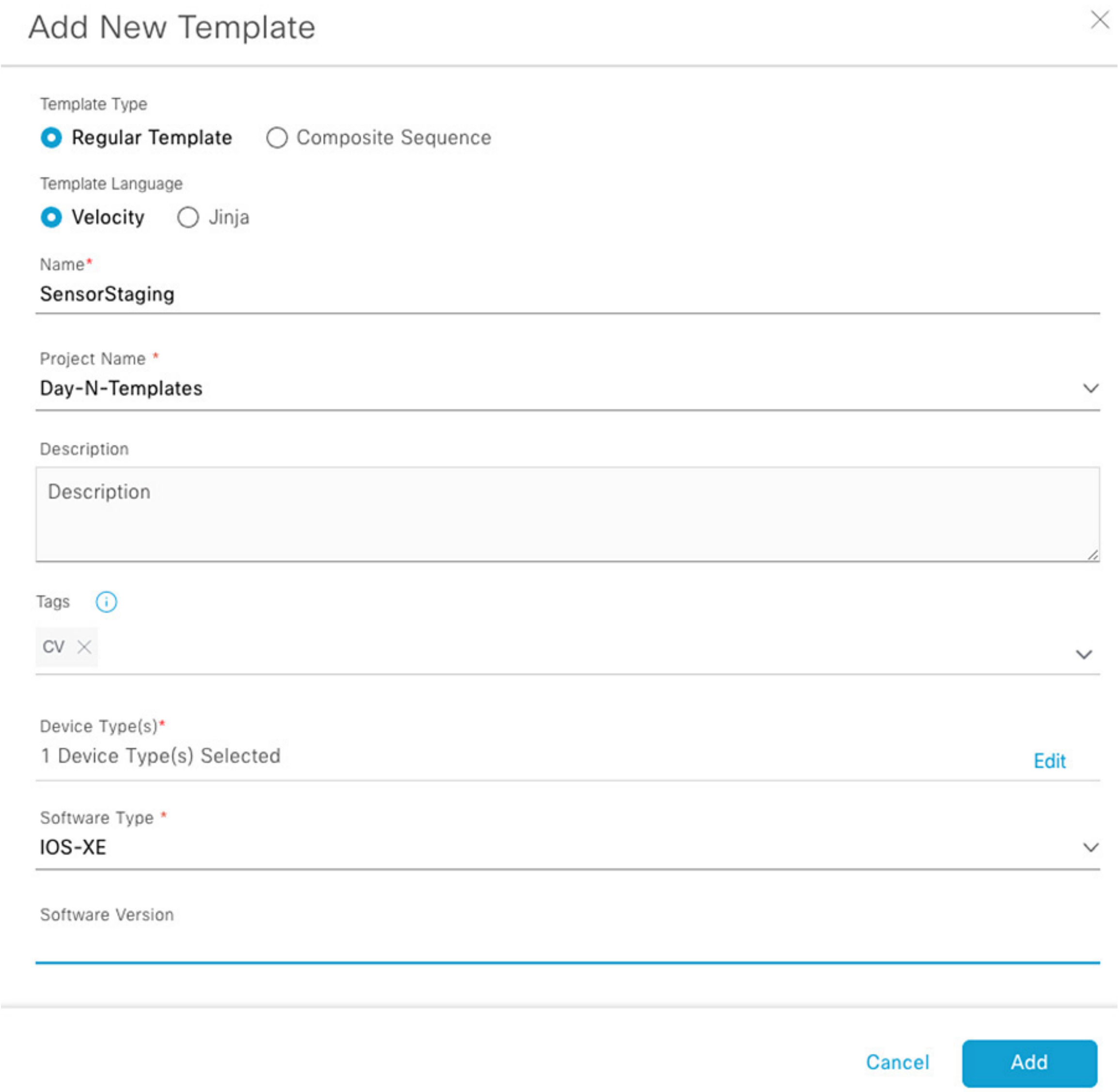
Configuration Preview

Device IP : 120.103.202.3

```
authentication convert-to new-style
ip radius source-interface Loopback0
aaa new-model
ip http max-connections 16
ip access-list extended ACL_WEBAUTH_REDIRECT
 40 deny ip any host 10.13.48.184
 500 permit tcp any any eq www
 600 permit tcp any any eq 443
 700 permit tcp any any eq 8443
 800 deny udp any any eq domain
 900 deny udp any eq bootpc any eq bootps
 exit
aaa session-id common
aaa group server radius dnac-client-radius-group
 server name dnac-radius_10.13.48.184
 ip radius source-interface Loopback0
 exit
aaa group server radius dnac-network-radius-group
 server name dnac-radius_10.13.48.184
 ip radius source-interface Loopback0
 exit
aaa accounting identity default start-stop group dnac-client-radius-group
aaa accounting update newinfo periodic 2880
aaa accounting exec default start-stop group dnac-network-radius-group
aaa authorization exec default local
aaa authorization network default group dnac-client-radius-group
aaa authorization network dnac-cts-list group dnac-client-radius-group
aaa authorization exec VTY_author group dnac-network-radius-group local if-authenticated
aaa authentication login default local
aaa authentication dot1x default group dnac-client-radius-group
aaa authentication login dnac-cts-list group dnac-client-radius-group local
aaa authentication login VTY_authen group dnac-network-radius-group local
dot1x system-auth-control
radius server dnac-radius_10.13.48.184
 address ipv4 10.13.48.184 auth-port 1812 acct-port 1813
 key ******
 retransmit 3
 timeout 4
```

6. Use tags to apply templates to selected devices.

**Figure 31 Cisco DNA Center Templates with Tags–1**



Add New Template

Template Type

● Regular Template ○ Composite Sequence

Template Language

● Velocity ○ Jinja

Name*

SensorStaging

Project Name *

Day-N-Templates

Description

Description

Tags

CV

Device Type(s)*

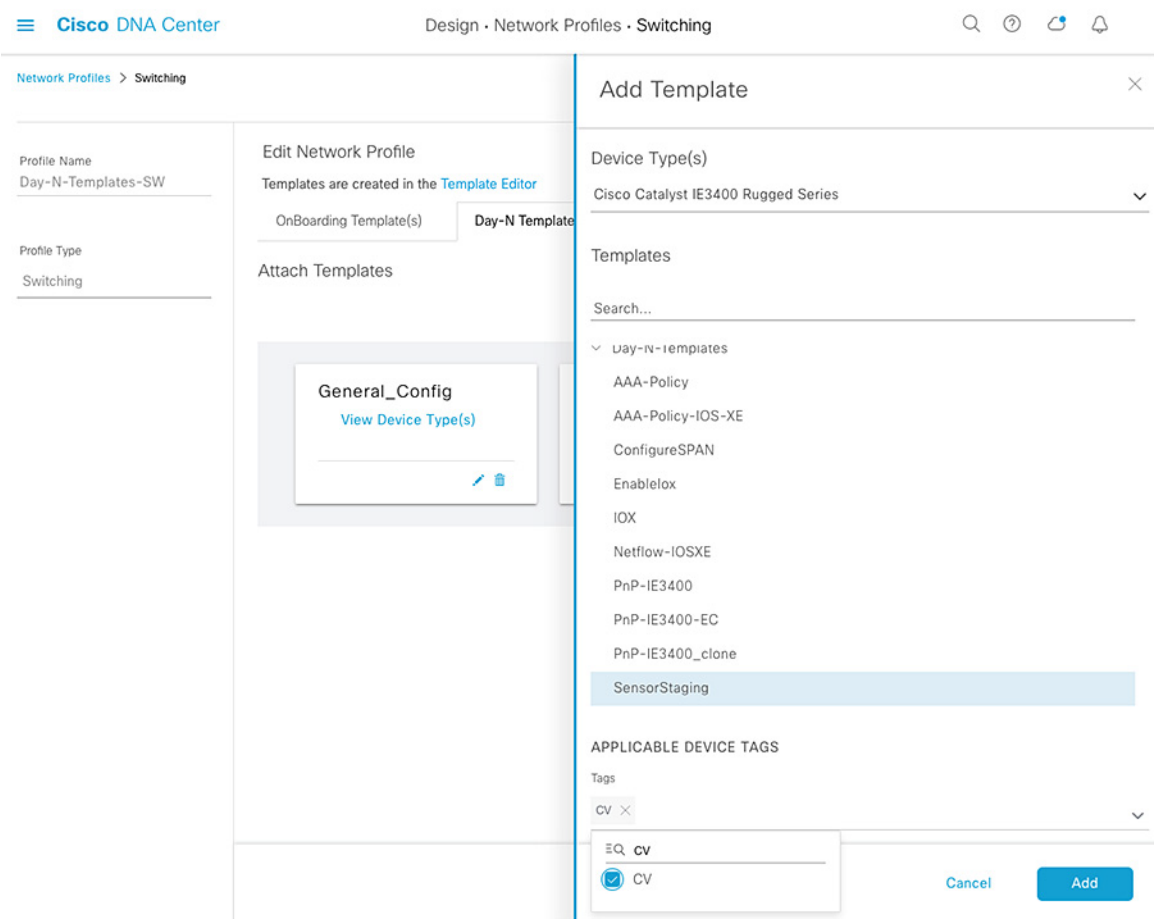
1 Device Type(s) Selected

Software Type *

IOS-XE

Software Version

**Figure 32 Cisco DNA Center Templates with Tags–2**



Cisco DNA Center | Design · Network Profiles · Switching

Network Profiles > Switching

Profile Name: Day-N-Templates-SW

Profile Type: Switching

Edit Network Profile

Templates are created in the Template Editor

OnBoarding Template(s) | Day-N Template

Attach Templates

General_Config
View Device Type(s)

Add Template

Device Type(s): Cisco Catalyst IE3400 Rugged Series

Templates

Search...

- Day-N-Templates
  - AAA-Policy
  - AAA-Policy-IOS-XE
  - ConfigureSPAN
  - Enablelox
  - IOX
  - Netflow-IOSXE
  - PnP-IE3400
  - PnP-IE3400-EC
  - PnP-IE3400_clone
  - SensorStaging

APPLICABLE DEVICE TAGS

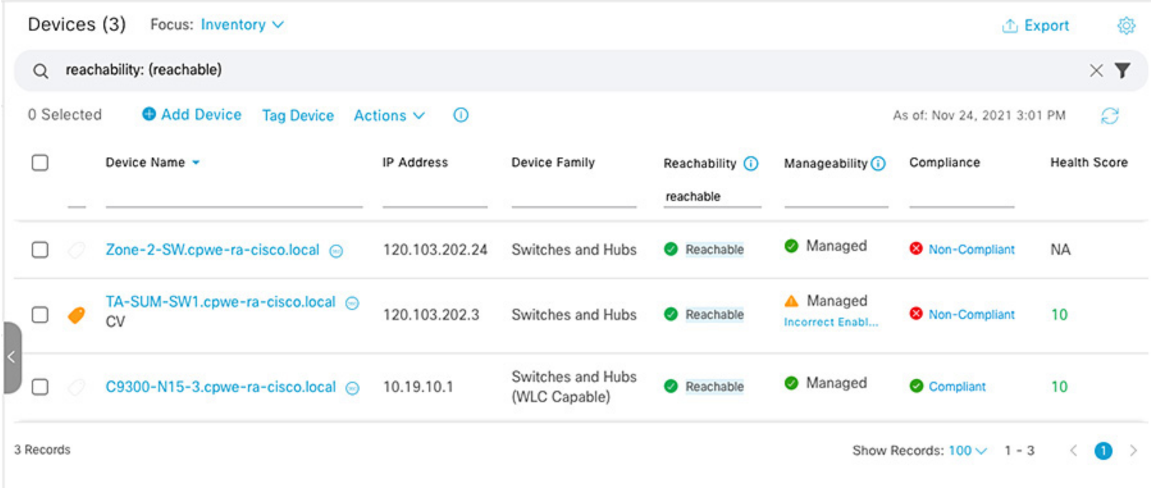
Tags: CV ×

cv

☑ CV

Cancel | Add

**Figure 33 Cisco DNA Center Inventory–Tagged Devices**



Devices (3) Focus: Inventory | Export

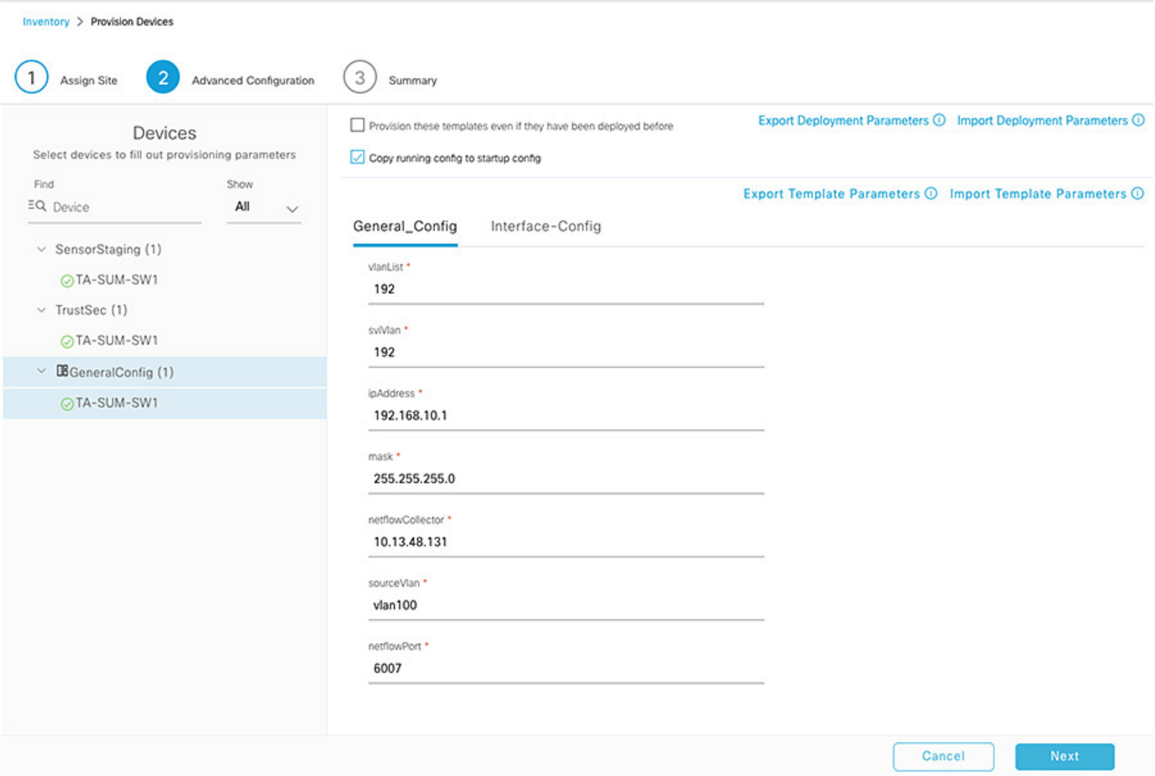
reachability: (reachable)

0 Selected | Add Device | Tag Device | Actions | As of: Nov 24, 2021 3:01 PM

| □ | Device Name | IP Address | Device Family | Reachability<br>reachable | Manageability | Compliance | Health Score |
|---|---|---|---|---|---|---|---|
| □ | Zone-2-SW.cpwe-ra-cisco.local | 120.103.202.24 | Switches and Hubs | ✓ Reachable | ✓ Managed | ✗ Non-Compliant | NA |
| □ | TA-SUM-SW1.cpwe-ra-cisco.local<br>CV | 120.103.202.3 | Switches and Hubs | ✓ Reachable | ⚠ Managed<br>Incorrect Enabl... | ✗ Non-Compliant | 10 |
| □ | C9300-N15-3.cpwe-ra-cisco.local | 10.19.10.1 | Switches and Hubs (WLC Capable) | ✓ Reachable | ✓ Managed | ✓ Compliant | 10 |

3 Records | Show Records: 100 | 1 - 3

**Figure 34 Cisco DNA Center Provisioning Templates per Tag**



Inventory > Provision Devices
1 Assign Site
2 Advanced Configuration
3 Summary
Devices
Select devices to fill out provisioning parameters
Find
Device
Show
All
SensorStaging (1)
TA-SUM-SW1
TrustSec (1)
TA-SUM-SW1
GeneralConfig (1)
TA-SUM-SW1
Export Deployment Parameters
Import Deployment Parameters
Export Template Parameters
Import Template Parameters
General_Config
Interface-Config
Cancel
Next

□ Provision these templates even if they have been deployed before

☑ Copy running config to startup config

vlanList * 192

sviVlan * 192

ipAddress * 192.168.10.1

mask * 255.255.255.0

netflowCollector * 10.13.48.131

sourceVlan * vlan100

netflowPort * 6007